



UNITED STATES MARINE CORPS
MARINE AIRCRAFT GROUP 12
FIRST MARINE AIRCRAFT WING, MARFORPAC
UNFT 37150
FPO AP 96603-7150

GruO P5270.1
ISC
AUG 27 1996

GROUP ORDER P5270.1

From: Commanding Officer
To: Distribution List

Subj: STANDARD OPERATING PROCEDURES FOR INFORMATION SYSTEMS
COORDINATOR (SOP FOR ISC)

Ref: (a) OPNAVINST 5239.1A
(b) MCO P5510.14
(c) FMFPACO P5230.13A
(d) RASC OKINAWA USERS MANUAL

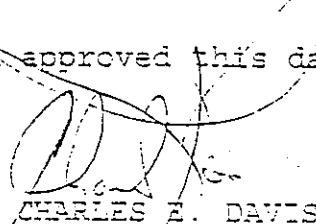
Encl: (1) LOCATOR SHEET

1. Purpose. To provide instructions, guidance and procedures for the Information Systems Coordinator at Marine Aircraft Group 12 (MAG-12), Marine Corps Air Station, Iwakuni, Japan. This SOP is intended to elaborate on regulations and guidance contained in the references.

2. Applicability. This order is applicable to this command and subordinate commands of MAG-12.

3. Recommendations. Recommendations concerning the contents of the SOP for ISC are invited. Such recommendations will be forwarded to the Commanding Officer (ISC) via the Chain of Command.

4. Certification. Reviewed and approved this date.


CHARLES E. DAVIS

Distribution: A

Copy to: CG, 1st MAW

LOCATOR SHEET

Subj: STANDARD OPERATING PROCEDURES FOR INFORMATION SYSTEMS
COORDINATOR (SOP FOR ISC)

Location: _____
Indicate location(s) of the copy(ies) of this Order.

SOP FOR ISC

RECORD OF CHANGES

Log completed change action as indicated.

SOP FOR ISC

CONTENTS

CHAPTER	TITLE
1	GENERAL
2	OPERATIONS
3	SERVICES
4	PROCEDURES

APPENDIX	TITLE
A	END USER COMPUTING (EUC) SOFTWARE
B	LAN ACCOUNT REQUEST
C	ABBREVIATED SYSTEM DECISION PAPER
D	ISC APPOINTMENT LETTER FOR SQUADRON
E	TASO APPOINTMENT FOR SQUADRON
F	GLOSSARY

SOP FOR ISC

CHAPTER 1

GENERAL

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	1000	1-3
PURPOSE	1001	1-3
MISSION	1002	1-3
RESPONSIBILITY	1003	1-3
ORGANIZATION	1004	1-3

SOP FOR ISC

CHAPTER 1

GENERAL

1000. GENERAL. The Information Systems Coordinator (ISC) is assigned by the Commanding Officer as a direct representative of MAG-12 for all internal and external information systems.

1001. PURPOSE. The purpose of this document is to provide information on the data processing resources available within MAG-12.

1002. MISSION. The mission of the ISC is to provide automated data processing technical assistance, to include hardware, software, and process implementation support, to personnel and units of MAG-12.

1003. RESPONSIBILITY. The ISC Officer is responsible for the efficient and effective management of information systems within the MAG.

1004. ORGANIZATION. ISC comprises the following functional areas:

1. Small Systems
2. Local Area Network
3. Software Development
4. Special information systems projects

SOP FOR ISC

CHAPTER 2

OPERATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	2000	2-3
CURRENT CONCEPT	2001	2-3
TECHNICAL TRAINING	2002	2-4
TECHNICAL LIBRARY	2003	2-4
CONSUMABLE SUPPLIES	2004	2-4
REQUESTS FOR SERVICES	2005	2-4
AUTHORIZED MAINTENANCE	2006	2-5
EQUIPMENT ACCOUNTABILITY	2007	2-5
EQUIPMENT ISSUE	2008	2-5
DARIC DISPOSAL/RECEIPT PROCEDURES	2009	2-6

SOP FOR ISC

CHAPTER 2

OPERATIONS

2000. GENERAL. The concept of an ISC was initiated to support the implementation of the ADPE-FMF Program. With the amount of computer equipment continuing to increase, it has become necessary to assign an ISC. It is essential that additional resources be applied to the management and support of equipment within the general and special staff.

2001. CURRENT CONCEPT. The current Marine Corps ADP support concept is structured around centralized policy formulation, technical direction, and acquisition under the Director, C4 Division, Headquarters Marine Corps. As the senior Marine Corps policy official for automated data processing, the Director is responsible for the procurement of mainframe ADPE, software and telecommunications, data processing equipment maintenance, and overall technical direction of Marine Corps-wide data processing functions. The current concept includes centralized management, regionally consolidated data processing service facilities and the continued use of established central design and programming activities for the development, operation, maintenance of Automated Information Systems and data communications.

1. Marine Corps Central Design and Programming Activity (MCCDPA's). There are three MCCDPA's which are located at Quantico, Virginia; Kansas City, Missouri; and Albany, Georgia. Each MCCDPA is organized, staffed, and equipped to analyze, design, develop, program, test, implement, and maintain Class I Automated Information Systems (AIS) as directed by CMC. The responsible areas for each MCCDPA as assigned by CMC are:

a. Quantico, Virginia, is responsible for the development, management, and publication of established ADP standards, and the newly implemented Standard Accounting and Budgeting Reporting System (SABRS).

b. Kansas City, Missouri, is responsible for the Joint Uniform Military Pay System (JUMPS) and associated AIS's.

c. Albany, Georgia, is responsible for all logistical AIS support.

2. Regional Automated Services Center (RASC) Camp Kinser, Okinawa, Japan. RASC Okinawa provides ADP support to the supporting establishment and the FMF commands within the Far East regions in accordance with the references. The RASC provides full processing support of Class I AIS's and general data processing service to users.

3. Remote Job Entry (RJE) Facility. The RJE of MCAS Iwakuni falls under the operational control of the Commanding Officer, MCAS Iwakuni. For technical direction, ADP guidance, and operational control of the mainframe services and Marine Corps Data Network (MCDN), control falls under RASC Okinawa.

4. Information System Management Office. Station ISMO is the primary office for information resource matters. Acting as the command focal point on all matters pertaining to coordination of information technology requirements, objectives, concepts, plans and policies, including establishing priorities with supporting and external data processing activities. ISMO's primary responsibility is support of tenant ADP functions.

2002. TECHNICAL TRAINING. All MAG-12 training is conducted through ISC. ISC has established a comprehensive technical training program. This training includes formal school training, classroom instruction, on-the-job training and cross training.

2003. TECHNICAL LIBRARY. ISC will establish and maintain a library of technical publications and manuals. At a minimum, one copy of all publications and manuals applicable to equipment and software maintained by the unit will be on hand. In addition, all syllabi for classes taught in the classroom, as well as all user guides for on-line products and applications will be maintained and made available to the user as required.

2004. CONSUMABLE SUPPLIES. All consumable supplies (i.e., paper, printer ribbons, diskettes, etc.) will be obtained through the individual section's supply system or ServMart. ISC is not charged with providing consumable supplies to units or sections.

2005. REQUESTS FOR SERVICES. Requests for services should be submitted to MAG-12 ISC at 253-6612. The MAG-12 ISC will process the request for further disposition if necessary.

2006. AUTHORIZED MAINTENANCE. 2nd echelon Maintenance on MAG-12 equipment will ONLY be performed by ISC personnel. Users of the equipment will perform 1st echelon preventive maintenance. Users are not authorized to move equipment to another section or unit.

2007. EQUIPMENT ACCOUNTABILITY. Computer equipment used by MAG-12 units and MCAS units must be appropriately identified and accounted for. Methods of accountability vary, those differences are listed below.

1. Table of Basic Allowance (TBA). This type of computer equipment has been purchased with Navy funds or "blue dollars." The equipment is accounted for by the appropriate unit's supply office.

2. Table of Equipment (T/E). This type of computer equipment has been funded and provided by Headquarters Marine Corps and designated to a unit's T/E allowance. The equipment is accounted for by the unit's supply officer and managed through the Marine Corps supply system.

3. Mainframe Peripheral Equipment. This equipment is the responsibility of the respective units' and shall be signed for accordingly. Items of this nature will be supported by RJE programs.

2008. EQUIPMENT ISSUE. ISC equipment is issued to users in one of two ways:

1. CMR-account. The MAG-12 ISC section will issue equipment/software to the Responsible Officer(RO) or sub-signer of an account in conjunction with Marine Corps Property after properly filling out and signing a 1348-1 Form. The 1348 is the transfer document from ISC to the receiving RO.

2. Individual Issue. The user will sign an Equipment Custody Receipt (ECR) card and take personal responsibility for the equipment. This method will be used when the user requires a temporary replacement until that section's equipment is fixed or replaced. Temporary loans are loans of computer components and are based upon availability and

necessity. Before requesting the temp-loan of items, all sections/units resources must be evaluated. Requests must be submitted in writing, with loans not exceeding thirty days unless authorized by the ISC Officer.

2009. DARIC DISPOSAL/RECEIPT PROCEDURES.

1. All serviceable equipment that the unit no longer requires needs to be reported to Defense Reutilization Resources Information Center (DARIC).
2. If the equipment is unserviceable the ISC will submit the serial number and NSN of the equipment to Marine Corps Property (MCP). MCP will then inform the ISC when the Defense Reutilization Management Office (DRMO) DD Form 1348 has been completed for the equipment.
 - a. Once the ISC has submitted the serial numbers to DARIC (through the Banyan Vines 3270 Telnet Functions), DARIC will send a report to the unit granting permission for disposal.
 - b. The DARIC Account holder will then process the report through the Supply Officer for generation of DRMO DD Form 1348. MCP will then contact the ISC section when the 1348's have been filled out and signed by the Supply Officer.
 - c. The ISC section will then take the equipment to DRMO for disposal.
3. DARIC can also be used for obtaining equipment. By searching through DARIC the ISC Section can locate available equipment from other units and request a transfer of the equipment.

SOP FOR ISC

CHAPTER 3

SERVICES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	3000	3-3
SOFTWARE DEVELOPMENT	3001	3-3
SMALL SYSTEMS	3002	3-4
LOCAL AREA NETWORK /MARINE CORPS DATA NETWORK SECTION	3003	3-5
SECURITY	3004	3-6
EDUCATION/TRAINING	3005	3-6

SOP FOR ISC

APPENDIX B

LAN ACCOUNT REQUEST FORM

LAN ACCOUNT REQUEST FORM

LAST NAME: _____ FIRST NAME: _____ MI: _____

RANK/GRADE: _____ SSN: _____

BILLET TITLE: _____ RTD: _____ / _____ / _____

DSN: _____ WORK SECTION: _____

DOES YOUR JOB REQUIRE THE NEED TO SEND E-MAIL OUTSIDE OF JAPAN?
YES OR NO (CIRCLE ONE)

JUSTIFICATION: _____

LAN ADMINISTRATOR USE ONLY:

INITIAL PASSWORD ASSIGNED: _____

ACID: _____

ACID DATE: _____

COMPLETION DATE: _____

- | | |
|--|--------------------------------|
| <input type="checkbox"/> LAN ACCOUNT | <input type="checkbox"/> CS |
| <input type="checkbox"/> SNADS | <input type="checkbox"/> IN |
| <input type="checkbox"/> DIR SER | <input type="checkbox"/> BMAIL |
| <input type="checkbox"/> ISC/TASO ADMINISTRATOR | |
| <input type="checkbox"/> LIST(S) (OFFICER, SNCO, CO, SGTMAJ, SQDN, RECALL) | |

NOTE: Attach a copy of the BTR/BIR to this request. NO LAN account will be established without the BTR/BIR attached. The purpose of the BTR/BIR is to verify the data of the LAN request with the data in the Marine Corps record system.

SOP FOR ISC

CHAPTER 3

SERVICES

3000. GENERAL. The ISC Section provides technical assistance to users and is the single point of contact for Marine Aircraft Group 12. If needed, the ISC will acquire assistance concerning the information systems used by the organization.

3001. SOFTWARE DEVELOPMENT. The ISC will provide services which include software support and development.

1. Computer software. Computer software is classified as proprietary or commercial software, public domain software, user developed software, or the software developed to support AIS Class I, II, and III.

a. Commercial Software

(1) Only those software packages contained in Appendix A will be authorized on Marine Corps owned End-User Computing Equipment (EUCE). Personal software, to include games, are not authorized for use on government EUCE, nor is Government software authorized for use on personal computers.

(2) Commercial software is not authorized for duplication unless expressly authorized by the vendor. Pirated or illegally duplicated software is not authorized on Government owned EUCE.

(3) Commercial software that is procured from other than authorized sources, and commercial software that violates U.S. copyright laws, is not authorized for use on Government EUCE.

b. Public Domain Software. Software available from public bulletin boards or other general software repositories is not authorized for use on Government owned EUCE. Public Domain Software is loosely managed and is susceptible to tampering and other sabotage such as "computer viruses."

c. Automated Information System (AIS) Software

(1) Class I applications operate on a mainframe computer system and are sponsored by a Headquarters Marine Corps Functional Manager (FM) and utilized by Marine Corps units.

(2) Class II applications operate on a mainframe computer and supports the local needs of a Headquarters staff agency, and FMF unit, or a Supporting Establishment (SE) organization. Class II applications are sponsored and maintained by RASC, Okinawa, Japan.

(3) Class III/IIB applications operate on a micro computer and are developed and supported locally by ISC and discussed further in Chapter 4. For assistance with this type of software contact the ISC section.

3002. SMALL SYSTEMS. The ISC Section provides installation and maintenance support for microcomputers, printers, and monitors.

1. Maintenance and Repair. At some point, all computer equipment will require some type of maintenance. When this occurs the user should contact the ISC section.

a. Trouble Calls. Maintenance will be initiated with a trouble call to the ISC. When an equipment malfunction is reported, repairs will be made as soon as possible based on the overall workload and the priority of the equipment effected. If repairs cannot be completed quickly, the user will be notified and given an estimate as to when the equipment will be back in service. If a temporary loan of equipment is required, it will be made available for a thirty (30) day period.

b. Preventive Maintenance. The user is responsible for preventive maintenance on the end user computer equipment and office machinery.

(1) Cleanliness of work spaces and the equipment are end user responsibilities. A routine of dusting keyboards and printers should be scheduled as part of preventive maintenance procedures.

(2) Ensure backup and recovery procedures are in place. Backups of all hard disks and floppy diskettes will be maintained in an area separate from the master diskettes and safe from environmental

hazards. Restore procedures must be tested periodically to ensure that backup procedures are adequate and to rotate the storage media used to hold backup information. Disk drives are more likely to fail than solid-state components.

(3) Unit/office SOP's should reflect good office practices that prevent food and drink from being spilled on the equipment, paper clips and staples dropped into keyboards, and other common occurrences that damage equipment.

2. Equipment installation. Requests for installation of hardware or software will be directed to the ISC. All installations will be coordinated with the user and ISC personnel.

3003. LOCAL AREA NETWORK/MARINE CORPS DATA NETWORK SECTION. The Okinawa Wide Area Network (CWAN) supports services associated with data communications for MCAS Iwakuni.

1. Marine Corps Data Network (MCDN). MCDN is the Marine Corps data communications network that provides the capability for data communication throughout the Marine Corps. The master computer connection called a "node" is located at RASC Okinawa with MCAS Iwakuni being a sub-node to that system. Requests for connectivity are described in Chapter 4. All problems with MCDN, (also called 3270) connectivity should be directed to the ISC section.

2. Defense Data Network (DDN). DDN is an a DoD communications system that provides the capability for data transmission world wide. Local DDN access is operated and maintained at Camp Zama, Japan. Use of DDN requires a microcomputer, single line phone, and a modem. Request for access to DDN must be submitted in writing and include name, rank, unit, building number, single line telephone number, and an account identification number (ACID) utilized for MCDN services. Send all requests to ISC Section.

3. Local Area Network (LAN). A LAN is a system of computers, printers and peripherals which are linked together by special hardware and software. LAN services allow users to share printers, data files and applications. Problems with access or connectivity should be directed to the ISC section.

4. Wide Area Network (WAN). A WAN is created when two or more LANs are connected to each other. On a broader scale, the WAN allows for connectivity outside MCAS Iwakuni. MAG 12's LAN is connected to RASC Okinawa's WAN to allow for Banyan Vines electronic mail and file transfers.

3004. SECURITY. Security covers all aspects of controlling and managing information resources. Physical security, data security, and system integrity are all managed as aspects of security. Security is covered in more detail in Chapter 4.

1. Computer Viruses. In today's world of LANS and WANS, it has become critical to monitor what system is attached to a network, what software will be used on that system, and most importantly, preventing unauthorized software from being introduced into a network. If a system is suspected of being infected, immediately contact the ISC section. Naval Criminal Investigative Service (NCIS) prevention measures are identified in Chapter 4.

2. Terminal Area Security Officer (TASO). Units requiring services of the mainframe computer system located at RASC Okinawa with a connection by remote terminal devices must have a TASO assigned. Duties of the TASO are described in Chapter 4.

3005. EDUCATION/TRAINING. Education/Training is given by the ISC section. It is designed to aid in the utilization of the government micro-computers. Formal classes are conducted at the classroom located at building 1450C. Training classes are provided for Marine Corps authorized software packages to include; MS-DOS, Lotus Smartsuite, Banyan, Local Area Network (user and administrative) software, and Terminal Area Security Officer (TASO). Users and sections can request classes on these subjects through the ISC section.

SOP FOR ISC

CHAPTER 4

PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	4000	4 - 3
MAINTENANCE SERVICE PROCEDURES.	4001	4 - 3
SECURITY	4002	4 - 4
LOCAL AREA NETWORKS	4003	4 - 9

SOP FOR ISC

CHAPTER 4

PROCEDURES

4000. GENERAL. This chapter provides guidance on the procedures established by The Information System Coordinator for Marine Aircraft Group 12.

4001. MAINTENANCE SERVICE PROCEDURES. Maintenance for computer equipment is managed by the ISC as follows:

1. Trouble Calls. When computer equipment requires maintenance, the user should contact the ISC section.

2. Service Procedures. Upon receipt of the trouble call, the ISC must:

a. Make a service visit to the unit. It is IMPORTANT to note that all personnel located in the vicinity of the "broken" equipment be familiar with the problem.

b. As a result of the service visit, the ISC section will decide if the equipment can be repaired on site, has to be removed from the site for further repair, or will require replacement. Replacement equipment is made available only when MAG-12 ISC has like items in stock. If the item needs to be removed from the site the following will apply:

(1) A first echelon equipment repair order (ERC) must be opened and the ISC will issue a receipt for the gear.

(2) The ISC will then attempt to repair the item in-shop.

(3) If the ISC cannot repair the item, depending on the item, the ISC will conduct one of the following:

(a) A second echelon ERC will be opened up and the item will be transferred to Station ISMC for repairs.

(b) If Station ISMO can not repair the item and it is not under warranty, the item will be shipped to Okinawa for repairs.

(4) If the item is under warranty, the item must be shipped to Camp Zama for repairs via the Transportation Management Office (TMO).

2. Automatic Data Processing Equipment (ADPE) Procurement and Requisition Procedures. The following procedures describe the process for procuring and requisitioning automated data processing (ADP) software and hardware equipment.

a. The user will submit a request to the ISC Officer (Appendix C.) The request will include the ADP requirements in general terms, a justification statement, an impact statement, unit price of the item, source of supply for the item, and a complete description of the item (to include model numbers, etc.)

b. The ISC section will conduct a site survey with the section Responsible Officer (RO), OIC, or SNCOIC to evaluate the requirements from a technical perspective, determine the specific items and amount required.

c. Upon approval by the ISC Officer, the requisition form, which will include the appropriation data information from the RO's account, along with the original request will be filed until assets are available.

(1) ADP requests will be approved based on the following criteria:

(a) The number of assets divided by the number of personnel in the section.

(b) The asset usage of personnel in the section:

1 A User - LAN account user only.

2 B User - LAN account user who occasionally uses word processing and/or spreadsheet programs.

3 C User - Frequent LAN account, word processing, spreadsheet, and database usage, and also program development.

(c) The current type assets available for the requirement (See Appendix C.)

d.. If the request is disapproved by the ISC Officer, it will be returned to the RO, OIC, or SNCOIC along with the reason(s) for disapproval.

e. Upon receipt of shipment, the ISC will contact the user and make arrangements for installation. The ISC section will then set up the equipment and install appropriate software, ensuring the system is operable.

f. Once the equipment is installed, the item will be assigned to the RO's property account for accountability.

g. Use of privately owned or leased personal computers to conduct official Marine Corps business in a government workplace or connected to a Marine Corps network is allowed only with the prior authorization of the Commanding Officer. Privately owned systems shall not be used to process classified data.

4002. SECURITY. Procedures for an effective security program are identified below:

1. Physical Security.

a. Workstations (microcomputers and remote terminals) and associated software will be located in areas which are easily secured after working hours and where surveillance is easily achieved.

b. Accurate inventory information and periodic reconciliation of serial numbers are basic tenets to a sound physical security program.

c. Physical security applies to systems and to individual components. Applications of security procedures will be at the lowest level.

2. Data Security. Data and the storage media it is stored on shall be controlled as required for the level of sensitivity or classification.

a. Unclassified Data. Data must be maintained in a file system that provides protection to the storage media and general correspondence filing procedures.

b. Sensitive Data. For Official Use Only and Privacy Act Information must be maintained in a secure area to prevent accidental disclosure or unauthorized personnel from accessing the information. Separate directories and password protected subsystem will be required when processing sensitive data on hard disks.

c. Classified Data. Confidential, Secret, Top Secret, and Special Compartmented Information will not be processed on workstations that have non-removable hard disk components, workstations that are connected to non-secure Local Area Networks, or workstations connected to any external network or modem. In those instances where classified processing must be processed on workstations configured with a non-removable hard disk, the entire workstation CPU must be treated as a classified information media device.

3. Hardware Security. A device which processes classified and/or unclassified sensitive information is subject to computer security procedures. Prior to use in processing classified information, workstations and all peripheral equipment will meet the standards of the categories for TEMPEST. TEMPEST is a term referring to the control of compromising emanations. The equipment will be either TEMPEST Certified, TEMPEST Accredited, or TEMPEST Approved. TEMPEST equipment is that which has been specially designed to meet stringent standards in order to reduce the amount of electromagnetic emanations.

a. TEMPEST Security. To maintain TEMPEST integrity, equipment may not be physically altered in any way to include drilling holes to secure the unit to a desk, opening the CPU to remove or add cards, or attaching non-TEMPEST certified peripherals to the standard configuration.

4. Software Back-up. To insure that no information is lost, back-up copies should be made for all important files. There are two types of back-ups that can be performed:

a. Partial. These back-ups are composed of only files that change daily. A partial back-up should be performed either daily or weekly depending on the size and importance of the information, and how often the information is updated.

b. Incremental. These back-ups usually go daily. This back-up is done by backing-up a different directory or program each day.

c. Full. These back-ups are composed of the complete hard drive(s) or programs and files being used and should be done either weekly or monthly.

4. System Integrity. System security implementation procedures will determine the success or failure of ADP system integrity.

a. System Accreditation. Systems must be accredited by a Designated Approval Authority (DAA). The Commanding General has been established as the DAA for 1st MAW in accordance with references (d) and (e). Accreditation is a formal statement by the DAA saying that all known vulnerabilities and risks associated with the system have been considered, and required countermeasures were implemented and found to be effective.

b. Risk Management. The objective of risk management is to achieve the most effective safeguards against deliberate or inadvertent disclosure of information:

(1) Unauthorized Disclosure of Information. This includes classified, privacy, resource, asset, proprietary or any other type of information deemed worthy of protection.

(2) Denial of Service or Use. Increasing dependence upon computerized systems dictates system availability. This objective relates closely to system reliability and continuity of operations aspects.

(3) Unauthorized Manipulation of Information. The system should be capable of ensuring the integrity of the data being handled.

(4) Unauthorized Use. The procedures should assist in protecting the system and in detecting unauthorized use.

5. Information Systems Coordinator (ISC). To help manage the squadron's accounts an ISC is appointed at the squadron level. The ISC must be appointed by the Commanding Officer, Director, or Officer-In-Charge of their unit utilizing the format in Appendix D.
6. Terminal Area Security Officer (TASO). To help enforce the squadron's security measures stated above, TASOs are assigned at Group levels. TASOs must be appointed by the Commanding Officer, Director, or Officer-In-Charge of their unit utilizing the format in Appendix E. Unit TASOs are assigned for each unit, section, or office within that department with a requirement to use mainframe (AIS) data files and job processes. TASO functions are as follows:
 - a. Must have access via a terminal to every host to which all of the administered users have access.
 - b. Must personally know every administered user. TASOs cannot ensure that access criteria are met and passwords are properly disseminated unless he knows the users to be administered. This requirement may necessitate the appointment of more than one TASO in larger organizations.
 - c. Must have physical access to all spaces where users gain access to AIS's.
 - d. Must have the ability/authority to add, vacate, suspend, or restore user ID's within their scope.
 - e. Problems or inquiries should first be directed and if possible resolved through the TASO. If a solution is not found to be possible, the TASO should contact the ISC section.

7. Computer Virus Prevention. A computer virus is a program that infects other data files or programs by modifying or destroying them. Like real viruses, computer viruses carry a genetic code, which in this case is recorded in machine language. The virus normally establishes itself on a disk and then silently infects every other program it can connect with. Computer viruses are becoming a common occurrence within the Government's small computer system environment. Given the increasing dependence of Marine Corps organizations on information stored and processed in small computers, the prudent

manager should understand the basics of what a computer virus is and adhere to the following controls in protecting their small computer systems:

- a. Ensure that an AUTHORIZED VIRUS PROTECTION PROGRAM is loaded onto the system during the boot process to scan for viruses on the hard drive, memory, and in the hidden system files.
- b. Ensure a scan program is installed to search floppy diskettes for any potentially contaminated diskettes.
- c. For Local Area Network (LAN) users, ensure Autoscan is loaded to check for viruses prior to logging into the LAN system.
- d. Do not introduce diskettes of questionable origin into a workstation that is connected by any network.
- e. Do not accept copied or pirated software. Observe copyright protection laws.
- f. Some viruses spread by attaching themselves to and/or modifying the COMMAND.COM file. Some versions of the Micro Soft Disk Operating System (MS-DOS) will allow you to protect against this type of virus by making the COMMAND.COM a "read only" file. For added protection, use a write protect tab on diskettes containing COMMAND.COM files.

NOTE: The above controls do not provide an absolute guaranteed method for protection against viruses; it simply makes it more difficult for a virus to spread.

g. ALL viruses identified by the scan on the users system should be identified to the ISC IMMEDIATELY to prevent further destruction of the data on the hard drive. The ISC section will assist in recovering or correcting contaminated data if possible. All viruses must be reported to the Information Systems Security Officer (ISSO) immediately.

4003. LOCAL AREA NETWORK (LAN). Requests for LAN within departments, units, or offices will be submitted to the ISC Officer. The request should include the requirements, justification, POC, location, and number of users requiring connectivity.

1. Standard. The current Marine Corps LAN standard is the Banyan Virtual Network Operating System (VINES).

2. Electronic Mail (E-MAIL). E-MAIL is a method of communicating information between individuals or organizations by means of computer-to-computer data transfer technology, normally in the form of text messages. E-MAIL is not a part of a formal record communication systems, nor is the application managed as a part of the Defense Communication system (AUTODIN).

3. Guidelines. The use of E-MAIL has been far reaching implications in the areas of communications and information security. The unrestricted use of E-MAIL could result in the misuse of current communications systems, or the potential loss of information currently managed per the Marine Corps records management directives. Use of E-MAIL within the Marine Corps will be regulated and controlled consistent with existing policies for other types of computer data transfer and records management standards. Therefore, the following guidelines have been established:

(a) Marine Corps policy will not be promulgated via E-MAIL. Marine Corps policy will continue to be established and promulgated through messages and the Marine Corps publications and directives system.

(b) Official Marine Corps positions may be cited in E-MAIL provided that they are being quoted from official correspondence which has been formally provided to the addressee(s).

(c) E-MAIL forwarded or received outside the chain of command will be considered informal unless prior coordination and agreement has been made between corresponding organizations. E-MAIL which is directive in nature between commands must be covered either by a formal agreement, or a higher command order governing types of correspondence authorized and detailed processing procedures.

(d) Per the Commanding Officer's policy letter, dated 21 Dec 1995 the following guidelines apply for all LAN Accounts:

(1) Officers and SNCO's will be provided a LAN account with world wide access upon request.

(2) Sgt's and below will be provided a LAN account with sufficient justification from the section OIC/SNCOIC. Sufficient justification is that the LAN account is necessary for the Marine to perform his daily MCS duties, where other means of communication (i.e., telephone, meetings, or memorandums) are inadequate. Where insufficient justification is provided for the LAN account, the OIC/SNCOIC will assist in the infrequent requirements of using the LAN, by forwarding the message for the Marine.

(3) Sgt's and below will be provided world wide LAN accounts only if there is an absolute necessity for the MCS task or unit task completion (i.e., Tech reps, and some deployable situations).

(e) If the intended use of an E-MAIL system is to include the transfer of information that would normally require the signature/authentication of the commander or a designated representative, commands will ensure the E-MAIL system provides for an electronic authentication scheme. In order to preclude

unauthorized personnel from "signing" for the commander, the scheme, at a minimum, should provide a level of protection equal to that afforded by current correspondence procedures. It must, at a minimum, provide a level of protection equivalent to the best current practice for electronic mail.

(f) E-MAIL may be referenced in official correspondence in the same manner that telephone messages and conversations are referenced.

(7) E-MAIL is restricted to official use only, as in the use of Government telephone and postal systems.

4. Organizational E-MAIL. Banyan E-Mail is any message or file transmitted to/from an authorized organizational mailbox intended for an organization not necessarily for a specific individual in the organization. This is comparable to traditional formal correspondence addressed generically to the commander or director of the organization.

5. Organizational Mailbox. An organizational mailbox is the E-MAIL address of an office, activity, or command, used to send/receive organizational E-MAIL only. More than one person may access this mail

box as authorized by the commander or head of the office owning the mailbox. The LAN profile for the organizational mailbox allows authorized users access to the E-MAIL and printer services of the LAN.

6. Individual Mailbox. An Individual Mailbox is the E-MAIL address of an individual to/from which individual E-MAIL is sent. Access to this mailbox is only by the individual to whom it is assigned, in accordance with established security procedures.

SOP FOR ISC

APPENDIX A

END USER COMPUTING (EUC) SOFTWARE STANDARDS

1. The approved software standards listed below have been selected by Headquarters Marine Corps for use throughout the command. Standards are established in order to ensure compatibility, reduce training costs, lessen the burden on EUC technical support personnel, and eliminate the need for the user to learn new software upon reassignment.
2. For use of EUC software other than listed below, the following procedure must be followed:
 - a. A request must be filled out and forwarded to MAG-12 ISC. This request must include the following information:
 - (1) Number of assets currently available to the user
 - (2) How additional assets will be used
 - (3) Why current assets are not adequate
 - b. After reviewing the request, the MAG-12 ISC will decide if the request is reasonable. If the request is reasonable the item will either be issued or placed on order.
 - c. If a request is disapproved, the requesting activity will be notified why the request was denied.
 - d. The MAG-12 ISC will keep copies of all requests for historic files whether they are approved or disapproved.
3. The interim or long-term use of non-standard software must be documented and approved by one of the following: HQMC; Department Heads; Fleet Marine Forces; CG FMFPAC FMFLANT; Reserve Forces; CG 4th CWT; others with Commanding General or Flag Level Commanders; CMC (C4I); and all others. The approval document must provide the reason the standard software listed below cannot be used.

SOP FOR ISC

4. Standards:

- a. Operating Systems: MS-DOS
PC-DOS
- b. Word Processing: LOTUS AMI PRO
- c. Data Base Management: LOTUS APPROACH
- d. Spreadsheets: LOTUS 123
- e. Graphics: FREELANCE GRAPHICS
- f. Utilities: NORTON UTILITIES
PC TOOLS

SOP FOR ISC

APPENDIX C

ABBREVIATED SYSTEM DECISION PAPER

1. Activity. Your unit and section.
2. Date prepared
3. Point of contact. Rank, name, billet and phone number.
4. Need. Outline the need for automation as related to specific elements of the activity's mission. Briefly summarize the functional requirements and information dependent tasks. Describe the current method and evaluate the impact on operations by maintaining the status quo capability.
5. Proposed Solution. Summarize the selected Financial Information Pointer (FIP) resource solution (functional requirements of the hardware and software) intended to satisfy the information processing need. Identify assumptions and constraints considered in the selection. Explain the acquisition strategy, indicating whether acquisitions will be competitive or noncompetitive and from what source they will be acquired. Indicate the milestone schedule of planned events, such as target dates for acquiring equipment and implementing various applications.
6. Other Alternatives Considered
 - a. Discuss the consequences if nothing is done to improve the current process.
 - b. Provide alternatives if full funding is not available for your proposed solution. What would you do if you only received half of the requested equipment.
7. Costs and Benefits. Summarize the projected costs (personnel, hardware, software, security mechanisms, and facilities) associated with developing each of the alternatives into an operational system. Identify expected benefits of each alternative such as improvements to functional support and cost savings. Give a cost and benefits rationale for selecting the recommended alternative.

SOP FOR ISC

8. Interface Considerations. Describe the planned or potential interface requirements with other systems, both internal and external to the organization. Indicate whether or not the project will be of an open system architecture. Indicate anticipated advantages, problems, and security vulnerabilities associated with system interfaces.
9. Testing. Describe the developmental, security, and operational tests, as applicable, to be conducted prior to deployment of the information resources.
10. Funding. Identify the source and type of funding expected to be used for the selected alternative. Give the current status of funding in support of the total expected life cycle costs of the selected alternative.
11. Garrison Property Reporting. All equipment must be accounted for on a Garrison Property account before it is delivered. In this section provide the Garrison Property account number, Responsible Officer's name, rank, and Phone number.
12. Other Comments. Include any additional information that will facilitate understanding and evaluation of the information system proposal. Training, security, privacy, maintenance, mobility and site preparation requirements should be addressed in the section.

9. Joint Signatures

Submitted:

(Program Manager)

Functional Requirement Validated:

(Functional Manager)

SOP FOR ISC

APPENDIX D

ISC APPOINTMENT LETTER

UNITED STATES MARINE CORPS
1ST MARINE AIRCRAFT WING, FMF PACIFIC
UNIT 37101
FPO AP 96603-7101

IN REPLY REFER TO:
S230
Section
Date

From: Appointing Officer

To: You (Include Rank First Middle. Lastname SSM/MOS USMC)

Subj: APPOINTMENT AS INFORMATION SYSTEMS COORDINATOR (ISC)

- Ref: (a) FMF PacO 5230.3F
(b) WgO 5230.10
(c) MCO 5510.14 ADP Security Manual
(d) MCO 5271.4A Electronic Mail Policy and Guidance
(e) IRM 5239-06 Data Access Security
(f) IRM 5239-04 Local and Wide Area Networks

1. Per references (a) and (b), you are appointed as the Information Systems Coordinator (ISC) for (your section), Unit, 1st Marine Aircraft Wing. You are to read and familiarize yourself with references (a) through (f). This appointment will remain in effect until you are formally relieved by the appointment of another ISC.
2. You will contact the Information Systems Management Officer (ISMO) to obtain a class seat for the required security training as the ISC (645-2301/3984).

Appointing Officer's signature
and printed name.

S230
Date

FIRST ENDORSEMENT

From: You (Rank First Middle. Lastname SSM/MCS USMC)
To: Appointing Officer, section

1. I have read and familiarized myself with the contents of references (a) through (f) in connection with my appointment as the 1st MAW, section, ISC. I further understand that I am required to attend ISC security training within 30 days of my appointment as the ISC.
2. My RTD is (date of RTD) and my phone number is (phone number).

Your signature and printed name.

SOP FOR ISC

APPENDIX E

TASO APPOINTMENT LETTER

UNITED STATES MARINE CORPS
1ST MARINE AIRCRAFT WING, FMF PACIFIC
UNIT 37101
FPO AP 96603-7101

IN REPLY REFER TO:
1510
XX/XXXXXXX
(DATE)

From: OIC
To: Rank/Rating Full Name SSN/MOS Branch of Service or Title
Subj: APPOINTMENT AS A TERMINAL AREA SECURITY OFFICER (TASO)
Ref: (a) MCO P5510.14
(b) IRM 5239-06 Data Access Security
(c) Computer Fraud and Abuse Act of 1986, Public Law 99-474
(d) IRM 5234-04 Naming Conventions

1. You are hereby appointed as a TASO for the (unit name and department identifier). Your TASO ACID is XXXXXX. You are to thoroughly familiarize yourself with references (a) through (d). This appointment will remain in effect until you are formally relieved.
2. You will contact the RASC Security Officer to obtain a class seat for the required security training as the TASO. Phone:

signature
typed name

5510
XX/XXXXXXX
(DATE)

FIRST ENDORSEMENT

From: Rank/Rating Full Name SSN/MOS Branch of Service or Title
To: OIC
Subj: TASO APPOINTMENT LETTER

1. I have read and understand references (a) through (d) and have assumed all duties in conjunction with my appointment as TASO. I further understand that I am required to attend security training as TASO for this unit.
2. My RTD is (date) and my duty phone number is phone # .

signature
typed name

SOP FOR ISC

Bulletin Board - A service which provides a computerized mechanism for information exchange.

BBS - Bulletin Board System.

Byte - 8 bits

Central Processing Unit (CPU) - Term used to represent the processing unit.

Classified Information - Information that must be protected to a particular security classification level due to its content.

CMR - Consolidated Memorandum Receipt for equipment.

Computer - A functional unit that can perform substantial computation, including numerous arithmetic operations or logic operations.

Computer Games - A software category best described as "any software package that does not provide a product which can be utilized in the environment for which the computer was purchased." Examples include: Tetris, Flight Simulator, Golf, Turbo Tax, etc.

Computer Network - A complex consisting of two or more inter-connected computers.

Cursor - A movable, visible mark used to indicate the position on which the next operation will occur on a display surface.

Data - A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

Database - A set of data, part or the whole of another set of data, and consisting of at least one file, that is sufficient for a given purpose or for a given data processing system.

Database Management System (DBMS) - An application that provides integrated organization, maintenance, storage and retrieval of information.

SOP FOR ISC

Data Circuit-terminating Equipment (DCE) - The equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line in a data station.

Data Communications - The transmission and reception of data.

Data Processing System - A system, including computer system and associated personnel, that perform input, processing, storage, output, and control functions to accomplish a sequence of operations on data.

Data Terminal Equipment (DTE) - That part of a data station that serves as a data source.

DD 250 - A DOD standard form used to document the acceptance of equipment.

DD-1149 - A requisition, invoice, and shipping document used to order equipment locally.

DD 1348-6 (FEB 85) - A DOD single line item requisition system document used to order parts in CONUS.

Debug - To detect, to trace, and to eliminate mistakes in computer programs or in other software.

Defense Data Network (DDN) - An international computer network managed by the DOD and used by all the uniform services.

Designated Approving Authority (DAA) - The Headquarters staff section, Commanding General, or Commanding Officer holding the authority to approve classified or sensitive processing at a certain level or below.

Digital - Pertaining to data that consists of binary digits.

Digital Computer - A computer that consists of one or more associated processing units and peripheral equipment and that is controlled by internally stored programs. A computer may be a stand-alone unit or may consist of several interconnected units.

Diskette - A flexible magnetic disk enclosed in a protective container. Synonymous with floppy disk.

SOP FOR ISC

APPENDIX F

GLOSSARY

1. This glossary contains working definitions to assist the ISC and the users they support. Terms are listed alphabetically and in some cases, repeated since the same function or device has more than one common name.

Access Time - The time interval between the instant at which an instruction control unit initiates a call for data and the instant at which the delivery of the data is completed.

Accreditation - The process used to request and obtain certification for a Marine Corps Automated Service Center computer system, or both, to process information at a particular security level.

ADP - Automatic Data Processing.

ADP System - Synonym for computer system.

ADPSO - Automated Data Processing Security Officer.

AIS - Automated Information System.

Analog -

a. Pertaining to the data consisting of continuously variable physical quantities.

b. Contrast with digital, discrete.

Analog Computer - A computer that processes analog data.

Analog Data - Data in the form of a physical quantity that is considered to be continuously variable.

Analog-to-Digital Converter - A functional unit that converts data from analog representation to a digital representation.

Artificial Intelligence - The capability of a device to perform functions that are normally associated with human intelligence, such as reasoning, learning, and self-improvement.

SOP FOR ISC

ASCII - American Standard Code for Information Interchange.

Asynchronous Transmission -

- a. Transmission in which the time of occurrence of the start of each character, or block of characters, is arbitrary; once started, the time of occurrence of each signal representing a bit within the character or block, has the same relationship to significant instants of a fixed time frame.
- b. The communications mode in which a start and stop bit are inserted between every eight bit word.

Automated Data Processing (ADP) - Data processing by means of one or more devices that use common storage for all or part of a computer program and also for all or part of the data necessary for execution of the programs; that execute user-written or user designated programs; that perform user-designated symbol manipulation, such as arithmetic operations, logic operations, or character-string manipulation; and that can execute programs that modify themselves during their execution. Automatic data processing may be performed by a stand-alone or by several connected units.

Backup - To make a copy of an entire file, floppy, hard disk, or other storage medium as a security measure.

Batch Processing -

- a. The processing of data or the accomplishment of jobs accumulated in advance, in such a manner that the user cannot further influence its processing while it is in progress.
- b. The processing of data accumulated over a period of time.

Baud - A unit of signaling speed equal to the number of discrete conditions or signal events per second. Normally measured in bits of data per second (bps).

Boot - The process of initializing the operating system.

Bug - A mistake or malfunction.

SOP FOR ISC

DOS - Disk Operating System.

Erasable Programmable Read-only Memory (EPROM) - Synonym for reprogrammable read-only memory.

EUCE - End User Computer Equipment.

File - A set of related records, treated as a unit.

File Server - On a network, the computer dedicated to the management and maintenance of network shared files.

Flexible Disk - Synonym for diskette.

Floppy Disk - Another term for diskette. Common formats include the 5 1/4" (low density - 360 KB, high density - 1.2 MB) and the 3 1/2" (low density - 720 KB, high density 1.4 MB).

Font - An assortment of characters of a given size and style.

Functional Manager (FM) - The section/person responsible for the control and management of a specific AIS.

Gigabyte - A unit of measure equal to one billion bytes.

Hard Drive - An assembly containing a sealed series of magnetic disks with the required read/write heads. Normal capacities start at 10 MB and above.

Hardware - (1) Physical equipment as opposed to programs, procedures, rules, and associated documentation. (2) Contrast with software

Impact Printer - A printer in which printing is the result of mechanical impacts.

Information Resource (IR) - A term that includes the people, ADPE and software, information systems and the information being managed by these resources.

Input-Output (I/O) - Pertaining to either input or output, or both. Peripheral devices are normally I/O devices, e.g. printer, monitors, disk drives, keyboards, etc.

SOP FOR ISC

IRM - Information Resources Management.

ISC - Information Systems Coordinator.

ISMO - Information Systems Management officer.

Job Control Language (JCL) - A problem-oriented language designed to express statements in a job that are used to identify the job or describe its requirements to a mainframe operating system.

Joy Stick - A lever with at least two degrees of freedom that is used as an input device, normally a locator.

JUMPS/MMS - Joint Uniform Military Pay System/Manpower Management System.

K - A contraction of kilo. When referring to storage or memory capacity, two to the tenth power, 1024 in decimal notation.

KBPS - Kilo Bits Per Second - A data transfer rate expressed as thousands of bits per second.

Keyboard - A device containing several rows of keys which are struck or "keyed" to enter input into a system.

Kilobyte (KB) - A unit of measure equal to one thousand bytes.

LAN - Local Area Network.

LAN Server - On a network, the computer dedicated to the network system software.

Line Printer - A device that prints a line of characters as a unit.

Management Information Systems (MIS) -

- (1) Management performed with the aid of ADP.
- (2) An information system designed to aid in the performance of management functions.

Marine Corps Data Network (MCDN) - An international network owned and managed by the Marine Corps.

SOP FOR ISC

Matrix Printer - A printer in which each character is represented by a pattern of dots. Synonymous with dot printer and dot matrix printer.

MCCDPA - Marine Corps Central Design and Programming Activity. Currently, three in the Marine Corps: Albany, GA.; Kansas City, MO.; and Quantico, VA.

Megabyte (MB) - A unit of measure equal to one million bytes.

MIMMS - Marine Corps Integrated Maintenance Management System.

MIS - Management Information System.

MISSO - Manpower Information System Support Office.

Modem - A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital signals to be transmitted over analog transmission facilities. Modem is a contraction of modulator-demodulator.

Monitor - The video display screen connected to a system. The terms CRT, VDT, terminal, console, display, monitor, screen, and video are synonymous.

MSDOS - Microsoft Disk Operating System.

Nanosecond - A unit of measure equal to one billionth of a second.

Network - See computer network.

Node - In a network, a point where one or more functional units interconnect transmission lines.

On-line -

(1) Pertaining to the operation of a functional unit when under the direct control of a computer.

(2) Pertaining to a user's ability to interact with a computer.

(3) Pertaining to the user's access to a computer via a terminal.

SOP FOR ISC

Operating System - Software that controls the execution of programs. An operating system may provide services such as resource allocation scheduling, input/output control, and data management. Operating systems are predominantly software.

Peripheral Equipment - Equipment external to the CPU which supports the operations of the computer.

Piracy - Pertaining to software, see Software Piracy.

Plotter - An output unit that presents data in the form of a two-dimensional graphic representation.

Pointer - An identifier that indicates the location of an item of data.

Point-to-Point Connection - A connection established between two data stations for data transmission. The connection may include switching facilities.

Polling -

a. On a multi-point connection, the process whereby data stations are invited one at a time to transmit.

b. Interrogation of devices for purposes such as to avoid contention, to determine operational status, or to determine readiness to send or receive data.

Preventive Maintenance - Maintenance performed specifically to prevent errors, faults, or problems from occurring.

Print Wheel - A rotating disk that presents characters at a single print position. Synonymous with type wheel.

Processor - In a computer, a functional unit that interprets and executes instructions.

Program - A sequence of instructions suitable for processing.

SOP FOR ISC

Programmer - A person who designs, writes, and tests computer programs.

Programming - The designing, writing, and testing of programs.

RAM - Random Access Memory.

Random Access - An access mode in which specific logical records are obtained from or placed into a mass storage file in a nonsequential manner.

RASC - Regional Automated Service Center. Currently, five in the Marine Corps: Camp Pendleton, CA.; Camp Lejuene, NC.; Camp Butler, Okinawa; MCAS Cherry Point, NC.; and MCAS El Toro, CA.

ROM - Read Only Memory.

Record - A set of related data or words treated as a unit, e.g., in stock control, each invoice could constitute one record.

Record Layout - The arrangement and structure of data or words in a record including the order and size of the components of the record.

Record Length - The number of words or characters forming a record.

Remote Access - Pertaining to communication with a data processing facility through a data link.

Remote Job Entry (RJE) - submission of a job through an input unit that has access to a computer through a data link.

RO - Responsible Officer.

RS-232 - A standard 25 pin plug used to connect either serial or parallel devices to systems or other devices.

SAERS - Standard Accounting Budgeting and Reporting System.

SASSY - Supported Activity Supply System.

SDLC - Synchronous Data Link Control. The communications protocol used by MCIN.

SOP FOR ISC

Scheduled Maintenance - Maintenance carried out in accordance with an established time schedule.

Sensitive Information - Unclassified information that requires restricted access. This category includes Privacy Act information, financial information for units/accounts with aggregate resources of \$100,000 or higher, and information that might prove embarrassing to the using unit, the Marine Corps, or the United States.

Serial Port - A port assigned to handle serial devices such as modems, graphic plotters, serial printers, etc.

SMU - Sassy Management Unit.

Software - Programs, procedures, rules, and any associated documentation pertaining to the operation of a system. Contrast with hardware.

Software Piracy - The acquisition of software you did not purchase, or the distribution of software to another person, in violation of the licensing agreement provided with the package.

Spreadsheet - An application which facilitates the creation, storage, and manipulation of primary numeric data and calculation of "what if" projections. An electronic ledger.

Surge Protectors - A device used to protect electrical equipment from surges in the electrical power by activating a quick blow fuse to sever the power connection.

Synchronous - Pertaining to two or more processes that depend upon the occurrence of a specific event such as common timing signal.

Synchronous Transmission - Data transmission in which the time of occurrence of each signal representing a bit is related to a fixed time frame.

System - In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions.

TASO - Terminal Area Security Officer.

SOP FOR ISC

TBA - Table of Basic Allowance.

T/E - Table of Equipment.

Telecommunications - The transmission of signals over long distances

TEMPEST - A set of specifications covering the electromagnetic emissions from, among other things, computers. The standard limits the allowable emissions from machines processing classified information.

TEMPEST Accredited - Denotes that a system or piece of equipment has been both certified and accredited to process classified information.

TEMPEST Certified - Denotes that a system or piece of equipment has passed the series of standard TEMPEST tests.

Terabyte - A unit of measure equal to one trillion bytes.

Time Bomb - A program which performs some destructive act triggered by a date or time.

Token - A device or control code held by users and used in conjunction with access control software.

Token Ring - A type of LAN operating system which passes a control code or "token" from station-to-station. Only the station holding the token ring can transmit data.

Trapdoor - Unpublicized gaps that legitimate programmers sometimes leave in their programs.

Trojan Horse - A program which appears useful but contains some destructive action. Free software may be a virus in disguise.

Turnaround Time - The elapsed time between submission of a job and the return of the complete output.

UDS - Unit Diary System.

SOP FOR ISC

Uninterruptable Power Supply (UPS) - A backup system consisting of generators or battery banks that provide the necessary voltage required to keep a system running during local power fluctuations or outages.

Validation - The checking of data for correctness or for compliance with applicable standards, rules, and conventions.

Verify - To determine whether a transcription of data or other operation has been accomplished accurately.

Virus - A self-replicating program that travels from computer to computer via network, telephone modem, or hand carry of infected media.

Wide Area Network (WAN) - A network generally defined as being spread out over an area larger than several units or a base.

Word Processing - An application which permits the entry, editing, and printing of textual material.

Work Station - Used to refer to a microcomputer system or terminal connected to another computer.

WORM -

a. A special type of virus which reproduces itself and moves throughout a program wiping out data and program code with access control software.

b. W.O.R.M - Acronym standing for write once, read many.