IRM 5239-10
W/CH 1

U.S. Marine Corps

SMALL COMPUTER SYSTEMS SECURITY

PCN 186 523910 00

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D.C. 20380-0001

IN REPLY REFER TO
5239/10
CCIS-45
23 MAY 1990

From: Commandant of the Marine Corps

Subj: SMALL COMPUTER SYSTEMS SECURITY

Ref: (a) MCO P5510.14
(b) P.L. 100-235, Computer Security Act of 1987
(c) MCO 5271.1

Encl: (1) IRM-5239-10

1. PURPOSE. To provide standards and guidance for managing and implementing the security requirements of Small Computer Systems as required by references (a) and (b).

2. AUTHORITY. This publication is published under the authority of reference (c).

3. APPLICABILITY. The guidance in this publication is applicable to all contractors and Marine Corps personnel responsible for the management and use of small computer systems. This publication is also applicable to the Marine Corps Reserve.

4. SCOPE

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized only by CMC (CC) on a case by case basis.

5. RECOMMENDATIONS. Recommendations concerning the contents of this technical publication should be forwarded to CMC (CCI) via the appropriate chain of command. All recommended changes will be reviewed upon receipt and implemented if appropriate.

6. SPONSOR. The sponsor of this technical publication is CMC (CCI).

J. A. STUDDS
By direction

DISTRIBUTION: PCN 186 523910 00

Copy to: 8145001

UNITED STATES MARINE CORPS
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VIRGINIA 22134-5001

IN REPLY REFER TO
5239/10 Ch 1
CSBT-8

MAY 0 3 1995

From: Commanding General

Subj: INFORMATION RESOURCES MANAGEMENT (IRM) SMALL COMPUTER SYSTEMS SECURITY

Ref: (a) MCO 5271.1A

Encl: (1) New page insert to IRM-5239-10

1. PURPOSE: To transmit new page inserts to the basic technical publication.

2. ACTION:

a. Remove page 2-1 to 2-6.

b. Insert new Chapter 2, pages 2-1 to 2-6.

3. SUMMARY OF CHANGES: This change brings the National Policy up to date on Tempest Countermeasures Review (TCR).

4. RECOMMENDATIONS: Recommendations concerning the contents of this technical publication should be forwarded to the Commanding General, Marine Corps Combat Development Command (via the appropriate chain of command) at the following address:

CG MCCDC
Director
Architecture and Standards Division - C491
3255 Meyers Avenue
Quantico, VA 22134-5048

5. FILING INSTRUCTIONS: This change transmittal will be filed immediately following the signature page of the basic technical publication.

6. CERTIFICATION: Reviewed and approved this date.

J.H. CHURCH
by direction

DISTRIBUTION: PCN 186 523910 00
Copy to: 8145001

UNITED STATES MARINE CORPS

Information Resources Management (IRM) Standards
and Guidelines Program

SMALL COMPUTER SYSTEMS SECURITY
IRM-5239-10

MAY 2 8 1990

Enclosure (1)

(This page intentionally left blank)

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change

(This page intentionally left blank)

PUBLICATION TABLE OF CONTENTS

Chapter Table of Contents

Chapter 1

GENERAL

(This page intentionally left blank)

Chapter 1

GENERAL

1.1. INTRODUCTION

1.1.1. Background. Low cost small computer systems and their benefits have resulted in a widespread use of these devices by the Marine Corps. These systems are used to support a variety of applications in areas such as word processing, personnel, pay, maintenance, supply, embarkation and intelligence, as well as locally identified requirements. The value of the information stored on these systems, as well as the cost of the equipment itself, has become an important security concern.

a. Information can be stolen (for personal gain or profit), misused, lost or modified (either accidentally or intentionally). The accidental loss, theft or modification of information costs the government thousands of dollars and many man-hours to recover each year, and in some cases cannot be recovered at all. Thus, appropriate safeguards must be maintained.

b. Small computers were originally developed for limited access, stand-alone, single user applications which did not require the use of internal hardware controls to prevent unauthorized access. However, the small computer system has advanced rapidly and is now frequently connected to networks and no longer limited to single user applications. Unfortunately, the development of security control measures has not kept pace. This fact makes them an easy target for theft, misuse, espionage, sabotage, accidental loss, and other unauthorized acts.

1.1.2. Purpose. This technical publication provides information, guidelines and procedures for implementing small computer systems security in accordance with the requirements set forth in the Marine Corps Automatic Data Processing (ADP) Security Manual, MCO P5510.14. The intent of this publication is to complement and amplify MCO P5510.14 in those areas unique to the security requirements of small computer systems.

1.1.3. Small Computer Systems. For the purpose of this technical publication, small computer systems are those systems generally referred to as personal, professional, portable, laptop, home, small business or desktop (including FMF-EUCE) computers. This definition includes word processing systems, office automation systems, and Local Area Network (LAN) workstations and servers.

1.1.4. Computer Security. Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs, data, facilities and

workplaces to assure the availability, integrity, and confidentiality of computer based resources and to assure that intended functions are performed without harmful side effects. In this document, computer security will be broken down and discussed in terms which relate more closely to small computer systems. Guidance will be presented in the areas of physical, software, information, and network security as they relate to the security requirements of small computer systems. The intent of this guidance is to ensure that the following security objectives are met:

a. Confidentiality of classified or sensitive information handled by the small computer system.

b. Integrity of information and related processes handled by small computer systems, from its origin through input, processing, and finally the output phase.

c. The availability of information when it is needed.

d. Accountability of persons accessing the data.

1.1.5. Who Should be Concerned. Computer security is not limited to any one individual or group of individuals. In today's Marine Corps, the evolution of small computer systems, either directly or indirectly, has an impact on the day-to-day activities of virtually every employee. With this in mind, the responsibility for protecting small computer systems and the information on them resides with every individual, beginning with the end user. Since end user computing places management of information in the hands of the individual rather than in a central data processing center, the individual must develop a security mind-set and be aware of the security needs of the small computer system environment. YOU can make a difference.

1.1.6. References and Definitions. A list of references is contained in Appendix A. A list of terms and corresponding definitions is provided in Appendix B. These appendices are provided to assist the reader in gaining an understanding of some of the references and terms unique to the field of computers and computer security.

Chapter Table of Contents

Chapter 2

COMMAND RESPONSIBILITIES

(This page intentionally left blank)

Chapter 2

COMMAND RESPONSIBILITIES

2.1. SECURITY POLICY. Due to the use and nature of small computer systems, every Command will implement a Small Computer Systems Security Policy to govern the management and use of small computer systems. Additionally, each command should incorporate into local security awareness training programs information unique to the security requirements of small computer systems. It is the responsibility of the command to ensure that managers and users of small computer systems adhere to the guidelines of the locally established security policy.

2.2. ROLE OF MANAGEMENT. Managers of small computer systems should implement, at a minimum, the guidelines set forth in this publication and those established by the local Small Computer Systems Security Policy. This does not mean that security measures are limited to those defined in this publication. Any additional measures which are reasonably based on the results of risk assessments and judgment of the manager should be taken to ensure that a proper level of security is maintained. Appendix C contains a checklist to assist in determining whether or not an appropriate level of security is being maintained.

2.3. ROLE OF THE USER. Every user of a small computer system is responsible for protection of the data which the system stores, processes or transmits. The user is also the first line of physical security for protection of that device from theft and unauthorized access. Appendix D provides a checklist to aid users in maintaining a proper level of security in their immediate workplace.

2.4. ACCREDITATION

2.4.1. Responsibilities. Commands will ensure that small computer systems under their purview are properly accredited in accordance with this Directive and MCO P5510.14, Marine Corps ADP Security Manual. Appendix E is provided to aid the manager in completing the accreditation process. Due to the large number of small computer systems in use and in an effort to reduce the paperwork and time involved in the accreditation process, group accreditations may be authorized under the following guidelines:

a. A group consists of a reasonably manageable number of computer systems.

b. The group must be limited to the confines of a unit, section or division within a command.

c. The devices must be configured similarly.

Ch 1

d. The devices must be used to process similar types of applications using similar software.

e. None of the devices in the group are used to process classified information. Devices processing classified information must be accredited on an individual basis.

f. The devices must be subject to the same threat environment.

2.4.2. Accreditation by the DAA. Accreditation is a formal statement by a Designated Approving Authority (DAA) stating that all known vulnerabilities and risks associated with a computer based system have been considered, and all cost-effective countermeasures have been implemented, tested and found to be effective. All computer based systems are to be accredited to the maximum specified level of sensitivity (Sensitive Unclassified, Confidential, Secret, Top Secret, National Cryptologic, SCI/Intelligence, SIOP-ESI) of the information that will be processed.

a. Accreditation Authority Levels. The DAA authority (organization exercising operational control in conjunction with the functional owners of the data) to accredit computer facilities is listed in reference (a). The DAA for all other computer based systems (e.g., AISs, mini-computers, micro-computers, word processors, office automation systems, local area networks) processing Classified or Sensitive Unclassified data is determined by the following data sensitivity levels:

(1) The DAA for Sensitive Unclassified data is vested in the Commanding Officer unless otherwise identified by another organization, functional manager or higher level authority stating ownership of the data or AIS. Sensitive Unclassified information is defined in the Computer Security Act of 1987 as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the Privacy Act of 1974.

(2) The DAA for Secret and Confidential (less SCI and Cryptologic) must be a Commanding Officer, Officer-in-Charge or equivalent.

(3) The DAA for Top Secret (less SCI and Cryptologic) must be a Commanding General, General Officer or equivalent.

(4) The DAA for SCI/Intelligence is the Defense Intelligence Agency. The DAA for Cryptologic Systems is National Security Agency. The DAA for SIOP-ESI is the Joint Chiefs of Staff (JCS). Accreditation requests for SCI/Intelligence systems are to be forwarded directly to Director, ONI (54).

Ch 1

Accreditation requests for Cryptologic systems are to be forwarded to COMNAVSECGRU. Accreditation requests for SIOP-ESI systems are to be forwarded to CMC (PP&O).

b. TCR. Before any computer based system that is identified to process classified information can be accredited, except those systems located on military bases within the U.S. that process data classified no higher than Secret, a Technical Countermeasures Review (TCR) must be submitted in accordance with OPNAVNOTE c5510 ser 09N/4C535007 dated 14 Apr 94. DAA's should not accredit systems to process classified information unless a current TCR submission is on file when required.

c. Reaccreditation. Computer based systems processing classified or Sensitive Unclassified information must be reaccredited at least every three years or whenever the system is reconfigured in a way which significantly changes the risks and vulnerabilities associated with it.

d. System Accreditation Labels. When a computer based system has been formally accredited by the DAA, a system accreditation label (sticker) will be placed on each device. Refer to Appendix E for guidance on ordering the accreditation labels and placement of the labels on the computer equipment.

2.4.3. Classes of Information. For the purpose of the accreditation process, information is divided into the following classes:

a. Classified Information. Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under E.O. 12356, or prior orders, DoD 5200.1-R, to require protection against unauthorized disclosure; and (c) so designated.

b. Sensitive Unclassified Information. Any information the loss, misuse, unauthorized access to, or modification of which might adversely affect U.S. national interest, the conduct of DOD programs, or the privacy of DOD personnel. Some examples of Sensitive Unclassified Information are:

(1) For Official Use Only - Requiring confidentiality of information of a sensitive, proprietary, or personal nature which must be protected against unauthorized public release.

(2) Financial - Requiring protection to ensure the integrity of funds or other fiscal assets.

(3) Proprietary - Requiring protection to protect data or information in conformance with a limited rights agreement or which is the exclusive property of a civilian corporation or individual and which is on loan to the Government for evaluation

or for its proper use in adjudicating contracts.

(4) Personnel - Requiring protection as stated in the Privacy Act of 1974.

c. Unclassified Information. Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse.

Chapter Table of Contents

Chapter 3

THREATS AND CONTROLS

(This page intentionally left blank)

Chapter 3

THREATS AND CONTROLS

3.1. PHYSICAL SECURITY. Physical security can be divided into two major categories. First are those measures taken to protect against natural disasters such as fires, floods, and power outages/surges. Second are those measures taken to protect against intruders.

3.1.1. Natural Disasters

a. Threats. The major area of concern for Small Computer Systems in this area is due to power outages and surges as a result of storms, brownouts, and equipment failure. Damages caused by these types of threats can cause thousands of dollars worth of damage to both the equipment and the information stored on them.

b. Controls. The following is a list of measures that should be considered to aid in minimizing the effects from these and other natural disasters:

(1) Use surge protectors.

(2) Schedule frequent backups of diskettes and hard disk drives (where appropriate).

(3) Save documents being worked on frequently (applies primarily to word processing).

(4) Locate equipment away from windows.

(5) Keep equipment elevated to prevent damage due to standing water.

(6) Use adequate fire protection measures (seek the advice of the local fire department to ensure proper measures are used).

(7) Institute a Disaster Recovery or Contingency Plan (See IRM-5239-09, CONTINGENCY PLANNING).

3.1.2. Intruders

a. Threats. Physical access must be restricted in order to protect data and equipment against common criminals, so-called activists, espionage or sabotage agents, vandals, and trusted persons engaged in any unauthorized acts. Small computer systems have been stolen and intentionally shorted out. Small computers are an especially attractive target for thieves.

b. Controls. Due to the current nature of personal computers, physical access control measures are considered to be the best method for denying unauthorized access. The following is a list of measures that should be considered to aid in reducing the threat from intruders:

(1) Place equipment in limited access areas. This includes the space surrounding equipment processing sensitive information that is under sufficient physical and administrative control to preclude an unauthorized entry or compromise.

(2) Ensure systems are not left unattended during normal working hours (i.e.-- secured during coffee breaks, lunch breaks, etc.).

(3) Use sign-in logs for systems used by multiple users.

(4) Use access rosters of approved users to identify authorized personnel.

(5) Use physical restraint devices to prevent removal of equipment.

(6) Ensure that when an office space is vacant during non-duty hours, doors are secured and access is controlled.

(7) Use a check list for securing the area at the end of the day.

(8) Use a device that can be installed in the power circuit to terminate power that can then be physically locked to prevent restoration of power to the equipment.

(9) Maintain accurate inventories of both hardware and software. These items should be listed by serial or plant property number.

For further information and guidance concerning physical security, refer to OPNAVINST 5530.14B, DON Physical Security and Loss Prevention Manual.

3.2. SOFTWARE SECURITY. The Marine Corps honors all licenses, copyrights, patents, restrictions and terms and conditions associated with commercial, proprietary computer software. Personnel are not authorized to copy (other than for backup), modify or transfer purchased computer programs. "Pirating" (making unauthorized copies of software) is a violation of copyright laws, and employees are subject to indictment and conviction if found guilty. Unauthorized copies are illegal even if they are used only for the government job and are never taken home for personal use.

3.2.1. Threats. A common practice on small computer systems is to backup software onto diskettes. The ease with which this is

done makes the theft or unauthorized use of government developed or procured software very inviting. The most common threat in this area is from the user who owns his own small computer system and believes there is nothing wrong with making copies of software packages for their personal use.

3.2.2. Controls. A vast majority of the software being used on small computer systems (primarily personal/desktop computers) in the Marine Corps falls into the category of off-the-shelf software. Most off-the-shelf software is proprietary or licensed and as such may not be distributed or copied without proper authorization. To ensure that government developed software is not misused or stolen and that the Marine Corps does not become liable for improper distribution of commercial software products, the following measures should be adhered to:

a. Ensure original (diskette) copies of software products are properly secured and accounted for in accordance with MCO P4400.150D, Consumer-Level Supply Policy Manual.

b. Periodically audit software inventory to verify holdings.

c. Ensure all authorized backup copies are properly secured and controlled by a cognizant authority.

d. Ensure users of software products understand they are not allowed to make copies for personal use or distribution by having them sign a document to that effect.

e. Ensure personnel checking out of the command or leaving their current assignment (civilian or military) do not make copies of commercial software for use at their next job.

3.3. INFORMATION SECURITY. The safeguarding of sensitive information is the topic of numerous publications and the basis for virtually all computer security requirements. The Privacy Act of 1974 provides guidelines for the protection of information as well as the types of information that can be made public under certain conditions. Additional publications such as the Computer Security Act of 1987 and MCO P5510.14 provide specific guidance on the requirement to maintain information security.

3.3.1. Threats. Information is one of the areas most frequently involved in fraud and abuse cases. Some of the more common threats are: the entering of unauthorized information, manipulation of authorized information, manipulating or improperly using information files and records, and creation of unauthorized files and records.

3.3.2. Controls. Information being processed on small computer systems in the Marine Corps today covers the spectrum from classified to Sensitive Unclassified and is considered to be a valuable commodity. As such, appropriate measures must be taken to ensure the safeguarding of this information. The proper

marking of magnetic media and computer output is addressed by MCO P5510.14 and OPNAVINST 5510.1. The following measures, coupled with the ones covered under physical security, should be considered to aid in providing adequate information security:

a. Position terminal screens and printers to minimize unauthorized viewing.

b. Properly secure the original source material and computer generated output.

c. Properly secure the magnetic media (diskettes, tapes, removable hard disks, etc.).

d. Encrypt the data.

e. Use password protection for sensitive files.

f. Ensure removable disks and diskettes are properly marked.

g. Use adequate audit trails to track data from the original source documents through its input into the system and its final output or disposition. Audit trails should include information on who was accessing/using the information at any given point during its existence.

h. Avoid storing sensitive data on non-removable media such as a small systems hard disk, unless the system is located in a controlled space.

3.4. ENVIRONMENTAL SECURITY

3.4.1. Threats. Although the range of environments that small computer systems will operate in has expanded greatly, they are still subject to certain types of common environmental hazards. Some of the more common threats to small computer systems are: poor electrical power, smoke from cigarettes, spilled liquids, extreme temperatures, etc.

3.4.2. Controls. Environmental threats are usually well known and easy to counter. Both the manager and user of small computer systems should consider the following measures, in conjunction with those measures previously identified, to aid in countering environmental threats:

a. Use dust covers on equipment not in use. Note: Do not cover equipment until after it has cooled off and never while it is turned on.

b. Do not operate equipment in temperatures and humidities which are outside of its indicated operating range. Check the user's manuals to determine what the operating ranges are.

c. Periodically clean equipment with appropriate computer cleaning products.

d. Do not eat, drink or smoke in the immediate area of a small computer system.

e. Keep equipment in good working order.

f. Do not locate equipment beneath water pipes.

g. Use antistatic pads and sprays to control harmful static electricity.

3.5. NETWORK SECURITY. Network security can be defined by those measures taken to prevent disclosure or modification of information through taps, manipulation of network interfaces, or components, and emanations. The guidelines identified previously for physical and information security apply to network security. There are additional requirements due to the distributed nature of networks. Because networks involving small computers can span several buildings, lines connecting elements of the network are exposed and difficult to provide physical security for. The additional requirements for network security are complex and beyond the scope of this publication. However, detailed guidance for network security is provided in IRM-5239-04, LOCAL AND WIDE AREA NETWORKS. Additionally, if a small computer system is connected to a mainframe host, then the user of that device must comply with the security requirements imposed by the host site.

3.6. PERSONNEL SECURITY. People are the most serious threat to computers and automated information. The unintentional errors people commit occur more frequently and cause more damage than do deliberate acts of sabotage. Unknowingly, people destroy or damage computers, related equipment, and software. Unwittingly, people enter incorrect data into the computer or erroneously alter data. Although many losses are caused due to unintentional acts, the intentional acts should not be overlooked. People intentionally damage, steal, or knowingly use automated information and computers for their own personal gain. It is important to remember that all security measures are vulnerable to users who have legitimate access.

3.6.1. Threats. Personnel threats are basically internal. People internal to an organization steal listings to sell for commercial use or personal gain. Computer supplies (disks, printer ribbons, paper, etc.) are attractive items for theft. The theft of a small computer itself is a problem. Some thefts are difficult to detect, such as the diverting of funds to erroneous accounts. Beyond theft of supplies and equipment is the abuse of assets. Common abuses include using the computer for personal business, browsing, preparing personal use software programs, and creating personnel use information, such as team rosters, scores, and handicaps.

3.6.2. Controls. It is up to the manager to provide leadership and supervision that will instill confidence and promote strong personal ethics among employees. The following recommendations coupled with strong leadership should be considered to aid in providing adequate personnel security:

a. Include both the organization's information security policies and the individual's responsibilities in information security training.

b. Publicize procedures to report security violations and irregularities.

c. Inform staff that unauthorized duplication and use of licensed software violates the law.

d. Indoctrinate new employees to their ethical responsibilities.

e. Conduct periodic security briefings for all personnel dealing with sensitive information.

f. Ensure personnel are aware that they are responsible for the products of the information systems they process.

g. After annual security training, require personnel to sign a statement that they understand their information security responsibilities.

h. Assign responsibility for the equipment and the information processed on it to users of small computer systems.

i. Encourage personnel to be involved in risk analysis and contingency planning.

j. Develop a software integrity policy that cautions against "software piracy", which is the illegal copying of licensed software for personal use. The policy should describe the circumstances in which vendor developed software can be reproduced and distributed.

k. Be alert to unusual employee behavior -- low morale, refusal to take leave, or personal problems that may indicate vulnerabilities which could lead to information security problems.

l. Be aware of computer output and whether unauthorized items (e.g., mailing labels, etc.) are being produced.

m. Stress to staff the importance of personal integrity and ethics, and encourage the reporting of suspected security violations.

3.7. ADMINISTRATIVE SECURITY. Some of the most frequently overlooked security measures that can be implemented are simple administrative procedures. Although these procedures tend to be simple in nature, they are sometimes the most important ones to enforce. Managers and users of small computer systems should ensure administrative procedures, such as those previously listed and the following, are closely adhered to:

a. Conduct periodic inventories of hardware and software products.

b. Ensure equipment is appropriately carried on an individual's property account.

c. Do not share passwords with anyone else.

d. Do not tape passwords to desks, walls, or terminals. Commit it to your memory.

e. Establish and enforce password rules and be sure everyone knows them.

f. If audit trail printouts are produced, review them regularly and frequently.

g. Use a filing system to keep track of removable disks and diskettes.

h. Ensure procedures are in place for laptop computers. These procedures should, at a minimum, address:

(1) Conditions under which they may be checked out

(2) Check in/out procedures and forms

(3) Traveling safeguards (i.e., - hand carry, don't leave in hotel rooms, airline policies, etc.)

Chapter Table of Contents

Chapter 4

SECURITY CONCERNS

(This page intentionally left blank)

Chapter 4

SECURITY CONCERNS

4.1. CLASSIFIED DATA. Although processing of classified information on small computer systems is possible, it may only be authorized under very strict guidelines. No small computer system will process classified information without adherence to the guidelines and appropriate authorization. Information and procedures required to obtain authorization for the processing of classified information are contained in IRM-5239-08, COMPUTER SECURITY PROCEDURES and in MCO P5510.14 (Marine Corps ADP Security Manual). These documents also provide guidance for the management of classified data.

4.2. PRIVATELY OWNED RESOURCES. Use of privately owned or leased personal computers (to include contractor owned computers), or Public Data Networks 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 or DAA. Privately owned small computer systems shall not be used to process classified data. The following guidelines should be considered when establishing a local policy for the use of privately owned or leased hardware in government spaces:

a. If personal resources are authorized, then a written Command policy should be established explaining the Government's liability for private property.

b. Compatibility of systems, data storage media, and other components should be considered and resolved based on the Government's needs when privately owned computers are brought into a Government office. Commands should consider requiring such equipment to conform to standards, based on office requirements, and verified to be virus free.

c. Commands should caution managers that all Government records and data created or processed on privately owned computers belongs to the Government and will remain with the Government even after a privately owned computer leaves the office or becomes inoperable. For this reason care must be taken to make sure that the information is accessible and compatible with the government owned computers.

4.3. VIRUSES. 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 reach.

4.3.1. Threats. A virus may be benign. However, more frequently than not, its purpose is malicious. Once a virus is in a system, it can do things such as: destroy files, lock-up networks, modify information, and even steal files by transmitting them to another location. Viruses can invade systems from several avenues. One of the main sources for viruses is software obtained from public bulletin boards. Another is from "free" software which is passed from one individual to another.

4.3.2. Controls. For most people, a computer virus sounds like something out of a science fiction novel. However, 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 (and that means all managers, not just those involved with data processing) should understand the basics of what a computer virus is and adhere to the following controls in protecting their small computers:

a. Use only Government acquired software that comes in factory sealed containers from reputable dealers or Marine Corps authorized software provided through proper distribution or requisitioning channels.

b. Privately owned commercial software and game software is not authorized.

c. Use only official U.S. Government authorized bulletin boards. It is imperative that the software from the bulletin board be tested for the presence of a virus by the individual or organization responsible for computer security matters. (Ensure that software downloaded from a bulletin board be downloaded only to a floppy diskette drive and not to permanently installed magnetic media.) In addition, the use of public domain freeware or shareware software is not authorized unless it comes from an official Federal Government sanctioned bulletin board and has been tested for the presence of a virus before use.

d. Do not accept copied or pirated software. Observe copyright protection laws.

e. When possible, use a write/protect tab on diskettes containing COMMAND.COM.

f. Before loading new software onto a system, create a backup copy of the existing environment that can be restored in the event a virus is later discovered. This may be needed since sometimes the only way to eliminate a virus is to reformat the hard disk.

g. Some viruses spread by attaching themselves to a "command.com" or other type of file. A feature of DOS 3.1 and

later versions will allow you to protect against this type of virus by making them read only files. The ATTRIB.EXE utility allows you to change the status of a file. To use ATTRIB.EXE to set the Read Only attribute on your "command.com" file, type the following at the DOS prompt:

ATTRIB +R COMMAND.COM

This will prevent the file from being overwritten or erased. To remove the Read Only attribute, type:

ATTRIB -R COMMAND.COM

Note: This does not provide a guaranteed method for protection against viruses; it simply makes it more difficult for a virus to spread.

4.4. CONTINGENCY PLANNING. The intent of contingency planning for small computer systems is to ensure that users can continue to perform essential functions in the event that services provided by their system are interrupted. IRM-5239-09, CONTINGENCY PLANNING, provides detailed guidance for the development of a contingency plan. The following additional guidelines are presented to aid in the development and implementation of a proper contingency plan:

a. The contingency plan should be written, periodically tested, and regularly communicated to all personnel.

b. Contingency plans must take into account backup operations, i.e., how information will be processed when the usual small computer system cannot be used, and the recovery of any information which is lost or destroyed.

c. The plan should address selected equipment breakdowns, such as a single printer servicing many stations.

d. Procedures and equipment should be adequate for handling emergency situations (fires, floods, etc.).

e. Store backup materials, including the contingency plan, in a secure and safe location away from the small computer system site.

f. The contingency procedures must be adequate for the security level and vital importance of the information processed.

g. Personnel should know what to do in case of an emergency and be familiar with the contingency plan.

Appendix A

REFERENCES

1. OMB Circular A-130, Mgmt of Federal Information Resources.

2. Public Law 93-579, The Privacy Act of 1974.

3. Public Law 97-255, Fed Mgr's Financial Integrity Act of 1982.

4. Public Law 99-447, Computer Fraud and Abuse Act of 1986.

5. Public Law 100-235, Computer Security Act of 1987.

6. DOD Directive 5200.28, Security Requirements for AIS's.

7. CSC-STD-005-85, Magnetic Remanence Security Guideline.

8. SECNAVINST 5239.2, DON AIS Security Program.

9. SECNAVINST 5370.2H, Stds of Conduct and Government Ethics.

10. OPNAVINST 5239.1A, DON ADP Security Program.

11. OPNAVINST 5510.1H, DON Information and Personnel Security Program Regulation.

12. OPNAVINST C5510.93, Navy Implementation of the National Policy on Compromising Emanations.

13. OPNAVINST 5530.14B, DON Physical Security and Loss Prevention.

14. GSA, FIRMR BULLETIN 30 dtd Oct 15, 1985.

15. MCO P5510.140, Marine Corps ADP Security Manual.

Appendix B

GLOSSARY

Accreditation: A formal declaration by the DAA that the AIS (including networks) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Automated Information System (AIS): An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Contingency Plan: A plan for emergency response, backup operations, and post-disaster recovery maintained by an organization as a part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan.

Designated Approval Authority (DAA): The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS.

Proprietary Software: Software which is owned by a private individual or corporation under a trademark, patent or copyright for the exclusive use and distribution by that individual or corporation. Normally a license agreement comes with the software which states the copyright conditions under which the software can be copied or distributed.

Surge Protector: A device inserted into the electronic circuit of computer equipment to protect the equipment from rapid fluctuations in the electrical current being provided to the device.

Appendix C

MANAGER'S CHECKLIST

1. The manager of small computer system assets should keep in mind not only the dollar value of the equipment but the intangible value of the information stored on the system as well. The security requirements for small computer systems and the information stored on them are often overlooked and neglected. The intent of this appendix is to provide the manager of these assets with a checklist that can be used to determine if the security measures currently being used are sufficient.

2. Manager's checklist:

		YES	NO
a.	Is a surge protector being used?	___	___
b.	Is a UPS being used?	___	___
c.	Are backups being made of magnetic media?	___	___
d.	Are backups being stored off-site?	___	___
e.	Is equipment located away from windows?	___	___
f.	Is equipment elevated to prevent water damage?	___	___
g.	Is equipment not located under water pipes?	___	___
h.	Is a CO2 fire extinguisher within 40 feet of the equipment?	___	___
i.	Is equipment located in a limited access area?	___	___
j.	Is a sign-in log used for multi-user systems?	___	___
k.	Is an access control log used to identify authorized users?	___	___
l.	Is a physical restraint device used to prevent removal of the equipment?	___	___
m.	Has a checklist for securing the area at close of business been posted?	___	___
n.	Are original copies of software products secured and properly accounted for?	___	___
o.	Are periodic software and hardware inventories conducted?	___	___
p.	Are backup copies properly secured and accounted for?	___	___
q.	Have personnel been counseled concerning misuse of proprietary and government developed software?	___	___
r.	Are monitors positioned to minimize unauthorized viewing?	___	___
s.	Is original source material and computer generated output properly secured?	___	___
t.	Is magnetic media (diskettes, tapes, etc.) properly secured?	___	___
u.	Is password protection used for files on multi-user systems?	___	___

* v.	Has the system been accredited?	___	___
* w.	Has a contingency plan been developed?	___	___
* x.	Has a security awareness program been implemented?	___	___

3. Once the manager has completed the above checklist, the number of yes answers should be counted and checked against the following table to get a general idea of the adequacy of security measures currently being used. The manager should be aware that this is not a foolproof method for determining the adequacy of security measures. The primary purpose of the checklist and the following table is to provide the manager with a better understanding and a heightened awareness of the security requirements for small computer systems.

* Note: If any of these three questions are answered no, the system does not meet the necessary adequate security measures, regardless of the score thus far.

Number of yes answers	General Appraisal
1 - 5	poor
6 - 10	fair
10 - 15	average
16 - 20	good
> 20	excellent

Appendix D

USER'S CHECKLIST

1. The individual user is the first line of defense in providing security for the small computer system and the information being processed on it. As such it is the responsibility of each user to keep abreast of the security requirements for the equipment and information under his control. Each user should review the following checklist periodically as a reminder of those actions that can be taken to maintain the security of the small computer system. Remember, you could be the next victim of a security breach.

2. User's checklist:

		YES	NO
a.	Are your diskettes secured?	___	___
b.	Have you made backup copies of important files?	___	___
c.	Do you make backup copies on a regularly scheduled basis?	___	___
d.	Are backup copies of critical files stored off-site (i.e.-- in another building or office)?	___	___
e.	Is your computer connected to a power source via a surge protector?	___	___
f.	Do you know where the nearest fire extinguisher to your workplace is located?	___	___
g.	Do you turn off or otherwise secure your computer when you are away from your workplace?	___	___
h.	Do you password protect important or sensitive files?	___	___
i.	Do you secure your original documents at close of business?	___	___
j.	Do you secure your workplace at close of business (i.e.-- computer off, lights out, door secured, etc.)?	___	___
k.	If you use a password, have you memorized it and not written it down on an unsecured piece of paper?	___	___
l.	Do you know what level of data (classified or Sensitive Unclassified) you process on your computer?	___	___
m.	Are you familiar with the directives or laws that require the protection of classified or Sensitive Unclassified information?	___	___

Appendix E

ACCREDITATION REVIEW AND DAA APPROVAL FORM

The accreditation survey contained in this appendix and the information contained and reported in Appendix C and D will provide sufficient documentation and guidance to allow the DAA to formally accredit small computer systems.

1. ACCOUNTABILITY:

a. This microcomputer is assigned to:

Name _____ Code _____ Phone _____

Equipment Location: Base _____ Bldg _____ Room _____

Computer acquisition Date (year): _____

b. Primary Equipment Identification:

Computer Manufacturer, type and model # _____

Computer Serial # (found on CPU) _____

c. Ancillary equipment used with the computer:

	Manufacturer	Type	Model	Serial Number
Monitor	_____	_____	_____	_____
Printer	_____	_____	_____	_____
Modem	_____	_____	_____	_____

Is the computer equipment plugged into a power strip? Yes__No__

Other Installed Devices and Peripheral Equipment (e.g. extra memory card, extra hard disk, terminal emulation board, 80287 math coprocessor, mouse, print buffer, etc...)

_____ _____ _____
_____ _____ _____

d. List commercially procured software held:

_____ _____ _____
_____ _____ _____
_____ _____ _____
_____ _____ _____

e. AIS's processed (Name and Sensitivity):

_____
_____
_____
_____
_____

2. ACCREDITATION SURVEY:

a. Major purposes of this system: (check all that apply)

____Word processing
____Graphics
____Data Base Management
____Spreadsheets
____File Management
____Desktop Publishing
____Project Management
____Electronic Mail
____Communications
____File Transfer
____LAN Services
____Other (list)
_____
_____

b. Types of data processed: (check all that apply)

Classified*	Sensitive Unclassified**	Unclassified
____Top Secret/SCI	____Privacy Act	(describe)
____Top Secret	____Financial/Budget	_____
____Secret	____Business Sensitive	_____
____Confidential	____Operational Sensitive	_____
	____Logistics/Supply	_____
	____Official Use Only	
	____National Interest	
	____Federal Programs	
	____Proprietary (Copyright protected)	
	_____	
	_____	

* If processing Classified data on a PC - compliance with all appropriate security directives is required.

** Not a complete list.

c. Check which best describes the configuration of the equipment and its environment:

_____MICRO COMPUTER ONLY - stand-alone micro (no connectivity)
_____MICRO TO LAN - stand alone-micro connected to a Local Area Network (LAN)
_____MICRO TO MAINFRAME - stand-alone micro computer with terminal emulator or modem connected to mainframe
  _____Read Only
  _____Upload/Download Capability
_____PORTABLE MICRO COMPUTER
  _____Used as stand alone only
  _____Used for TAD, at home or off Government property
    _____Connected by modem to Government-owned mainframe
    _____Name and location of mainframe_____
    _____Word Processor Only (with or without terminals
_____OTHER _____

	Yes	No
d. Is a modem or terminal emulator connected to PC? If yes, is it ever used:	___	___
(1) To download classified data (If yes, contact CSSO)?	___	___
(2) In manual answer mode?	___	___
(3) In automatic answer mode (where the other end controls the intermachine transaction, as with a bulletin board)?	___	___
If yes, is this system protected by security access software?	___	___

e. List authorized users (include person PC is assigned to):

Name _____ Code _____ Phone _____
Name _____ Code _____ Phone _____
Name _____ Code _____ Phone _____
Name _____ Code _____ Phone _____

NOTE: Changing users does not require a new accreditation form; however, the CSSO must update the file copy of this form to reflect changes

3. COST ASSESSMENT:

a. What is the hardware replacement value? _____

b. What is the software replacement value? _____

c. What is the data replacement value? _____
Replacement or recreation (approximate only)

4. COUNTERMEASURES:

	Yes	No
a. Is the system protected by security access software? (If NO, continue with section b.)	___	___
(1) Software Name: _____		
(2) How often are passwords changed? _____		
b. Is the PC securely fastened to a desk or table?	___	___
c. Is the system in a room that is locked after normal working hours?	___	___
d. Are software, disks and tapes locked up when not in use?	___	___
e. Is the original vendor software backed up?	___	___

f. Data files are backed up? Daily ___ Weekly ___ Other: _____

5. CONTINGENCY PLAN:

Check and complete the appropriate section:

a. ____ A contingency plan is required for this system because an unplanned disruption of services would have a critical impact on mission accomplishment.

(1) In the event of a disruption of services, with respect to this system, all work will be performed on similar system(s) at base _____ bldg _____ room _____ using backup software.

(2) Original software and backup of file data is located at base _____ bldg _____ room _____.

b. ____ A contingency plan is not required for this system because an unplanned disruption of service would not have a critical impact on mission accomplishment.

6. ACCREDITATION COMPLIANCE AND REVIEW:

Check each statement that reflects compliance:
(mark N/A where applicable)

_____Procedures are in place which emphasize positive discovery of violations through audit and review.

_____Procedures exist to report violations to the individual or office responsible for computer security.

_____Procedures exist to ensure that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but no more.

_____Organizational structure minimizes the potential for fraud waste or abuse of computer resources (checks and balances).

_____Internal audit program exists (inspections, internal controls) which reviews computer security procedures.

_____Command personnel responsible for the security of classified information are involved with computer security personnel to ensure classified information is processed and stored on PC's in accordance with classified security regulations.

_____Classified diskettes are labeled with USMC standardized labels or pre-labeled color coded diskettes are used.

_____System is labeled with highest data sensitivity level handled.

_____Classified and sensitive unclassified files are stored on removable hard disks or floppy diskettes.

7. FORMAL ACCREDITATION. The following page contains a sample of the formal accreditation statement. This accreditation statement expires immediately once the micro:

a. Changes configuration (changes in section 2.c above),

b. Increases its capabilities in section 2.a above or upgrades data sensitivity levels in section 2.b above, or

c. Is moved to another location.

8. ACCREDITATION LABELS. When a standard computer configuration (system unit, monitor, keyboard, and printer), or peripheral devices cabled to the system unit have been formally accredited, a system accreditation label (sticker) that specifies the highest level of system sensitivity will be placed on each device in a conspicuous place. The rectangular block on the label will reference the DAA's accreditation letter and approval date. System accreditation labels are available through normal Marine Corps supply channels. Accreditation labels may be ordered using the following specifications:

a. "System Accreditation Label - SENSITIVE UNCLASSIFIED", NAVMC 11180, SN 0000-00-006-9700, Pad of 50 labels.

b. "System Accreditation Label - CONFIDENTIAL", NAVMC 11181, SN 0000-00-0006-9720, Pad of 50 labels.

c. "System Accreditation Label - SECRET", NAVMC 11182, SN 0000-00-006-9740, Pad of 50 labels.

d. "System Accreditation Label - TOP SECRET", NAVMC 11183, SN 0000-00-006-9760, Pad of 50 labels.

e. "System Accreditation Label - SCI", NAVMC 11184, SN 0000-00-006-9780, Pad of 50 labels.

ACCREDITATION STATEMENT

Date: _____

Subj: ACCREDITATION OF THE (Organization Name), MARINE CORPS BASE, (City, State) FOR THE STORAGE AND PROCESSING OF (Classified Level, Sensitive Unclassified, or Unclassified) DATA

1. References: MCO P5510.14, Chapter 11
MCO 5271.1
IRM-5239-08, Computer Security Proced

2. I have carefully considered the actual and potential threats to, and vulnerability of, the computer system(s) located in (room, building), and their associated peripherals and remote teleprocessing terminals (if applicable). Weighing the threats and vulnerabilities against the operational requirements and the security measures which have been implemented and/or planned in the area of physical, personnel, hardware/software, procedural and communications/emanations (if applicable) security, I have determined that the operation of (organization name) computer systems is in the best interest of Marine Corps operations and its mission.

3. Accordingly, under the authority granted me in the references, I have this date accredited the above system(s) to store and process data at the subject level.

4. Signatures

_____
Equipment Custodian

_____
Date

_____
Computer System Security Officer

_____
Date

_____ _____
Accreditation Authority (DAA) (Date)

COMMENTS/REVISIONS

Technical publications under the Information Resources Management (IRM) Standards and Guidelines Program (MCO 5271.1) are reviewed annually. Your comments and/or recommendations are strongly encouraged.

IRM Tech Pub Name: _____

IRM-____-___ (Number) Date of Tech Pub: _____

COMMENTS/RECOMMENDATIONS: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Name/Rank: _____(optional)

Unit: _____(optional)

Mail To: Commandant of the Marine Corps (Code CCIS)
Headquarters, United States Marine Corps
Washington, D.C. 20380-0001