

U.S. Marine Corps



COMPUTER SECURITY PROCEDURES

5239/08A

CSBT-8

From: Commandant of the Marine Corps

Subj: COMPUTER SECURITY PROCEDURES

Ref: (a) DODD 5200.28

(b) SECNAVINST 5239

(c) MCO P5510.14

(d) MCO 5271.1

Encl: (1) IRM-5239-08

1. PURPOSE. To provide guidance and amplification on the requirements contained in references (a) through (c) for compliance with the computer security program. Detailed procedures and guidance relating to the accreditation process, contingency planning, small computer systems and data access security will be addressed in separate technical publications.

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

3. APPLICABILITY. The guidance contained in this publication is applicable to all contractors and Marine Corps personnel responsible for the use of equipment which is designed, built, operated and maintained to collect, record, process, store, retrieve, and display information. This standard is 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 MCCDC (AS) on a case by case basis.

5. 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 Myers Avenue

Quantico, VA 22134-5048

6. SPONSOR. The sponsor of this technical publication is MCCDC (AS).

DISTRIBUTION: PCN 186 523908 00

Copy to: 8145001

UNITED STATES MARINE CORPS

Information Resources Management (IRM)
Standards and Guidelines Program

COMPUTER SECURITY PROCEDURES

IRM-5239-08A

Encl (1)

(This page intentionally left blank)

RECORD OF CHANGES

Log completed change action as indicated.

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

(This page intentionally left blank)

PUBLICATION TABLE OF CONTENTS

Chapter 1

GENERAL

Section 1. INTRODUCTION	1.1. 1-3
Section 2. PURPOSE	1.2. 1-3
Section 3. SCOPE	1.3. 1-3
Section 4. DEFINITION	1.4. 1-3

Chapter 2

PROCEDURAL SECURITY

Section 1. HISTORICAL REVIEW	2.1. 2-3
Section 2. CURRENT PERSPECTIVE	2.2. 2-3
Section 3. MANAGEMENT CONSIDERATIONS	2.3. 2-3

Chapter 3

PERSONNEL SECURITY

Section 1. INFORMATION	3.1. 3-3
Section 2. SENSITIVE DUTIES	3.2. 3-3
Section 3. BACKGROUND INVESTIGATION	3.3. 3-4
Section 4. SECURITY BRIEFING	3.4. 3-4
Section 5. SECURITY DEBRIEFING	3.5. 3-5
Section 6. DECLINATION	3.6. 3-5

Section 7. PERSONNEL AWARENESS	3.7. 3-5
--------------------------------------	----------

Chapter 4

PHYSICAL SECURITY

Section 1. INFORMATION	4.1. 4-3
Section 2. PHYSICAL SECURITY PRINCIPLES	4.2. 4-3
Section 3. SECURITY OF REMOTE DEVICES	4.3. 4-4
Section 4. SECURITY REVIEWS	4.4. 4-4
Section 5. EFFECTS OF MAGNETISM	4.5. 4-5

Chapter 5

HARDWARE SECURITY

Section 1. IMPORTANCE OF HARDWARE SECURITY	5.1. 5-3
Section 2. SUPPORT FOR TRUSTED SYSTEMS	5.2. 5-3
Section 3. SPECIAL CONSIDERATIONS	5.3. 5-5

Chapter 6

SOFTWARE SECURITY

Section 1. GENERAL REQUIREMENTS	6.1. 6-3
Section 2. TYPES OF SOFTWARE	6.2. 6-3
Section 3. ACCESS CONTROLS	6.3. 6-4

Section 4. SOFTWARE DEVELOPMENT	6.4. 6-7
Section 5. DATA BASE MANAGEMENT SYSTEM	6.5. 6-10
Section 6. UTILITY SOFTWARE	6.6. 6-10
Section 7. LEAST PRIVILEGE	6.7. 6-10
Section 8. TRUSTED COMPUTER SYSTEMS	6.8. 6-10
Section 9. SOFTWARE CERTIFICATION	6.9. 6-11

Chapter 7

COMMUNICATIONS SECURITY (COMSEC)

Section 1. INFORMATION	7.1. 7-3
Section 2. PROVISIONS OF ENCRYPTION EQUIPMENT	7.2. 7-3
Section 3. PROTECTION FROM IMPROVISED COMSEC	7.3. 7-4
Section 4. COMSEC PLANNING	7.4. 7-4

Chapter 8

EMANATIONS SECURITY (TEMPEST)

Section 1. APPLICABILITY	8.1. 8-3
Section 2. INFORMATION	8.2. 8-3
Section 3. TEMPEST TERMINOLOGY	8.3. 8-3
Section 4. RESPONSIBILITIES AND PROCEDURES	8.4. 8-4
Section 5. TEMPEST CONTROLS	8.5. 8-4
Section 6. FILTERED POWER	8.6. 8-5
Section 7. TEMPEST COUNTERMEASURES	8.7. 8-5
Section 8. PROTECTED DISTRIBUTION SYSTEM	8.8. 8-5

Chapter 9

CLASSIFIED PROCESSING

Section 1. INFORMATION	9.1. 9-3
Section 2. APPLICABLE TERMS	9.2. 9-3
Section 3. TEMPEST COUNTERMEASURE REVIEW (TCR) REQUIREMENT	9.3. 9-4
Section 4. SYSTEM ACCREDITATION/LABELS	9.4. 9-6
Section 5. CLASSIFIED MEDIA MARKING	9.5. 9-6

Chapter 10

TECHNICAL VULNERABILITY REPORTING

Section 1. INFORMATION	10.1. 10-3
Section 2. BACKGROUND	10.2. 10-3
Section 3. APPLICATION AND SCOPE	10.3. 10-3
Section 4. REPORTING PROCEDURES	10.4. 10-3
Section 5. NISAC REPORTS/BULLETINS	10.5. 10-4
Section 6. PRODUCT EVALUATION	10.6. 10-4

Chapter 11

NETWORK SECURITY

Section 1. INFORMATION	11.1. 11-3
Section 2. DATA NETWORKS	11.2. 11-3
Section 3. MINIMUM REQUIREMENTS	11.3. 11-3

Section 4. NETWORK ACCESS	11.4. 11-3
Section 5. NETWORK PROTECTION	11.5. 11-4
Section 6. DIAL-UP ACCESS	11.6. 11-4

APPENDICES

A. GLOSSARY OF ACRONYMS AND TERMS	A-1
B. REFERENCES	B-1
C. CLASSIFIED MEDIA AND EXTERNAL LABELS	C-1
D. COMPUTER LOG-ON WARNING SCREEN	D-1
E. SENSITIVE UNCLASSIFIED INFORMATION	E-1
F. SECURITY MODES OF OPERATION	F-1
G. TEMPEST COUNTERMEASURE REVIEW (TCR) (U)	G-1
H. TECHNICAL VULNERABILITY REPORT (DoD)	H-1

Chapter Table of Contents

Chapter 1

GENERAL

Paragraph Page

Section 1. <u>INTRODUCTION</u>	1.1. 1-3
Section 2. <u>PURPOSE</u>	1.2. 1-3
Section 3. <u>SCOPE</u>	1.3. 1-3
Section 4. <u>DEFINITION</u>	1.4. 1-3

(This page intentionally left blank)

Chapter 1

GENERAL

1.1. INTRODUCTION. This publication provides information, guidelines, procedures, and label requirements previously addressed in MCO P5510.14 and related directives that are pertinent to administering computer security. Excluded from this publication are data access security, the accreditation process (computer security plans, risk assessment, ST&E, accreditation statement) and contingency planning which are contained in separate technical publications.

1.2. PURPOSE. This publication is intended for both technical and functional users and discusses computer security considerations for large scale main-frame systems down to the microcomputer and network level. The key consideration in protecting computer systems or, more importantly, the sensitive data they process is for users and managers to develop a security mind-set.

1.3. SCOPE. The safeguarding of sensitive information against unauthorized access, modification, destruction, or denial of use is a computer security issue that requires the greatest degree of coordination and cooperation among all levels of command. In that regard, this publication will address the computer security disciplines which include personnel, administrative, physical, hardware, software, data, communications and emanations security measures and techniques.

1.4. DEFINITION. Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs, data, facilities and workspaces to assure the availability, integrity and confidentiality of computer-based resources and to assure that intended functions are performed without harmful side effects. Refer to Appendix A for a glossary of acronyms and terms pertaining to computer security.

Chapter Table of Contents

Chapter 2

PROCEDURAL SECURITY

Paragraph Page

Section 1. <u>HISTORICAL REVIEW</u>	2.1. 2-3
Section 2. <u>CURRENT PERSPECTIVE</u>	2.2. 2-3
Section 3. <u>MANAGEMENT CONSIDERATIONS</u>	2.3. 2-3
Separation Of Duties	2.3.1. 2-3
Delineation Of Responsibilities	2.3.2. 2-4
Security Indoctrination & Training	2.3.3. 2-4
Controlled Zone Environment	2.3.4. 2-4
Protection Of Documentation	2.3.5. 2-4
Organizational Placement Of The Computer	
Systems Security Officer (CSSO)	2.3.6. 2-4
Security In Life Cycle Management	2.3.7. 2-5
Control Of Networked Computer Systems	2.3.8. 2-5
Contingency Planning	2.3.9. 2-5
Risk Management	2.3.10. 2-5
Security Of Computer Media	2.3.11. 2-6
Accreditation By The Designated Approving Authority	2.3.12. 2-6

Computer Fraud And Abuse Act Of 1986	2.3.13. 2-8
Computer Security Reporting Procedures	2.3.14. 2-8

(This page intentionally left blank)

Chapter 2

PROCEDURAL SECURITY

2.1. HISTORICAL REVIEW Recognition of the importance and the necessity for Automated Information System (AIS) security and internal computer controls in the U.S. Government and the Department of Defense (DoD) is still evolving. U.S. legislation attempting to establish adequate methods of accounting and internal control dates back over 30 years. DoD Directives have attempted for over 15 years to improve the situation. Despite these efforts for improvement, technical innovation and programmatic implementation have not kept pace with the requirement.

2.2. CURRENT PERSPECTIVE During the last five years, computer use has increased exponentially. Technology has continued to evolve providing more users the opportunity to access computers and data bases. As a result, the threat to National Security information and other sensitive data has also increased proportionally. It is only recently that there has been a coordinated response by government and industry in support of improving AIS security. Media coverage of computer crime, espionage, and youthful "hackers", coupled with Public Law 100-235, "Computer Security Act of 1987" and the establishment of the National Computer Security Center (NCSC), has raised the level of computer security awareness in government, industry, and the general population. This revitalized awareness has elevated the subject of computer security from the sole domain of the computer specialist to one of national concern.

2.3. MANAGEMENT CONSIDERATIONS Procedural security is most closely associated with the management function of control as it relates to any of the different sized computer facilities (i.e., ADP site, Network Front-End Processor (FEP), Remote Job Entry (RJE), Departmental, mini-computers, microcomputers (PC's) and LAN server), supporting software, maintenance and entry/output accountability. It is at those points in the process where control passes from one function, element, or individual to another, that control can be lost. The purpose of this chapter is to alert managerial, operational, and user personnel of these vulnerabilities and, where possible, to prescribe procedures and techniques which can be applied to improve controls and reduce risks.

2.3.1. Separation Of Duties It is necessary from a security standpoint that key duties be separated so as to preclude any one person from gaining the opportunity to adversely affect the automated system. Procedural checks and balances must be built into manual interfaces so that deviations can be detected and reported to the appropriate Computer Systems Security Officer (CSSO), Terminal Area Security Officer (TASO), or Network Security Officer (NSO).

2.3.2. Delineation of Responsibilities Duties, responsibilities, privileges, and specific limitations of

all personnel involved in the operation of a computer facility processing sensitive information must be specified in writing and periodically reviewed by management or security personnel.

2.3.3. Security Indoctrination & Training Some of the most effective features of a security program are training and indoctrination. The Computer Security Act of 1987 requires government agencies to provide information on computer security awareness and acceptable practices. Computer security awareness encompasses formal and informal training to insure that all personnel involved in the use and management of computer resources understand and can implement their respective security responsibilities for safeguarding Sensitive Unclassified data derived from computer systems. Awareness training must be provided to new personnel, refreshed annually, and tailored to the types of responsibilities within the computer environment. In addition, personnel processing classified information must be indoctrinated with all applicable classified directives.

2.3.4. Controlled Zone Environment All operations within a controlled zone environment will be safeguarded and classified to the highest level of processing in accordance with applicable regulations or directives. This includes personnel, access lists, documentation, storage, equipment, and processing.

2.3.5. Protection Of Documentation The safeguarding of all documentation supporting mission critical applications and systems programs and their interaction is vital to effective security. Protection should be extended to all documentation revealing the logic, methodology, or instructions for system use. This includes, but is not limited to the following:

a. Software development documents (such as, system and logic diagrams, decision tables, program code, test data, data editing, error detection, test, and verification).

b. Debug routines and output (such as, core dumps, memory snapshots, trace routines), and vendor software instructions for loading and executing programs.

c. Documentation pertaining to software, system errors, or flaws (such as, security violation reports, generic system flaws, justifications for software or modification, or other software maintenance requirements).

2.3.6. Organizational Placement Of The Computer Systems Security Officer (CSSO) The CSSO

is the key individual responsible for security related matters and should report directly to the head of the organization. The CSSO should not report to any manager or supervisor that is responsible for keeping a system operational once a security problem has been discovered. This is to insure a sense of objectivity in the decision making process with regards to operations. The position of the CSSO (officer, enlisted, or civilian employee) can either be full-time or part-time and should depend upon the facility or organization size, and the level of processing sensitivity.

2.3.7. Security In Life Cycle Management (LCM) Security planning is an essential part of any program, system, development project, or procurement action. Computer security addresses each phase of the system life cycle. As defined in the LCM manual (MCO P5231.1) and augmented with the System Development Methodology (SDM) process, computer security requirements are dictated by the system being developed, the security mode being implemented and the degree of trust under which the system must operate. Security is relative to all other requirements of the system. As defined in DOD 5200.28-STD, all computer resources designed, developed and procured, that process or handle classified or Sensitive Unclassified information, shall implement as a minimum Class C2 functionality (controlled access protection which includes a user-ID, password, audit trail and memory clearing before reuse). See Appendix B for reference to LCM and related computer security directives.

2.3.8. Control Of Networked Computer Systems The increased operational flexibility of teleprocessing systems and their remote nature increases their vulnerabilities and the opportunity for exploitation. Computer facility management must ensure that security measures are in place and that only authorized users enter the system, manipulate data, and receive output. The audit trails of networked software should be capable of identifying all user-IDs and time of access including sign-on/sign-off. Guidance for Local and Wide Area Networks is contained in IRM-5239-04.

2.3.9. Contingency Planning Computer facility managers must ensure that sufficient copies of files, documentation, and other supporting material essential to recovery and continued processing of mission essential applications are secured in a readily available location. Conversely, end users should also maintain emergency plans to allow essential functions to continue in the event their automated support becomes unavailable due to any unforeseen circumstances. Detailed information and procedures are contained in IRM-5239-09, "CONTINGENCY PLANNING" and IRM-5239-16, "LOCAL AREA NETWORKS DISASTER PLANNING." (under development)

2.3.10. Risk Management The most effective means of protecting automated systems handling classified and/or Sensitive Unclassified information is through risk management procedures. Because each computer facility and operating environment is unique, management must identify those resources to be protected and analyze the risk of espionage, sabotage, damage and theft to determine the minimum level of protection. The objective of risk management is to achieve the

most effective safeguards against the following deliberate or inadvertent acts.

a. Unauthorized Disclosure of InformationThis includes classified, National Defense, privacy, procurement, proprietary, financial or any other defined types of sensitive information.

b. Denial of Service or UseIncreasing dependence upon computer systems dictates uninterrupted availability. This objective relates closely to system reliability, continuity of operations and continuation of mission, and includes events that require manual intervention.

c. Unauthorized Manipulation of InformationThe system should be capable of ensuring the integrity of the data being stored or processed.

d. Unauthorized PersonnelSystems are especially susceptible to exploitation by unauthorized personnel during scheduled or unscheduled system start-up, shutdown, or failure. Therefore, detailed logs, records, or other documentation of operational status at the time of failure are essential to provide audit trails and minimize the possibility of system compromise.

2.3.11. Security Of Computer MediaComputer media consists of any substance or material on which data is represented or stored and which is used for input and/or output to an automated system.

a. This includes magnetic tapes, disks (including removable hard disks), floppy disks, cassettes, paper tapes, punched cards, magnetic cards, CRT displays, hard copy output, core storage units, mass memory storage units (removable and fixed), printer ribbons, and computer output microfilm/microfiche.

b. Computer media on which classified information is stored must be controlled, safeguarded and labeled according to the highest classification level of data they have ever contained.

c. Refer to Appendix C for procedures relating to accountability, labeling, degaussing and destruction of classified data and media. Additionally, Appendix E identifies and addresses the requirements for the protection of Sensitive Unclassified data and media.

2.3.12. Accreditation By The Designated Approving Authority (DAA) Accreditation is a formal statement by a 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 C. 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 the Commanding Officer, Officer-in-Charge or equivalent.

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

(4) The DAA for SCI/Intelligence is the Defense Intelligence Agency. The DAA for Cryptologic Systems is the 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). 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. Tempest Countermeasures Review (TCR) Before any computer-based system that is identified to process classified information can be accredited, a TCR must be conducted (except those systems located on military bases within the U.S. that process data classified no higher than secret) in accordance with OPNAVNOTE c5510er 09N/4C535007 dated 14 Apr 94. There are some exception to the rule dealing with processing classified data on military bases within the U.S., please refer to the above OPNAVNOTE for instructions before trying to accredit a system. DAA's should not accredit systems designated or acquired to process classified information unless a Certified Tempest Technical Authority (CTTA) has conducted or validated a TCR. Refer to Chapter 9 and Appendix G for details.

c. Reaccreditation Computer-based systems processing classified or Sensitive Unclassified information must be accredited at least every three years or whenever the system is reconfigured in a way which significantly changes the risks and vulnerabilities associated with it. The Accreditation Process is addressed in a separate technical publication and includes the necessary guidance to allow a DAA to accredit a computer-based system.

2.3.13. Computer Fraud And Abuse Act Of 1986 The requirements of this Act (P.L. 99-474) are applicable to all personnel having access to automated system resources. Management must ensure that users of computer-based systems are aware that government owned or leased resources are for official use only. Guidance on taking appropriate action against offenders of the law is contained under General Standards of Conduct in DODD 5500.7D and SECNAVINST 5370.2H.

a. Warning Banner All computer-based systems are required to have a log-on warning screen mechanism in place to ensure that users are aware of their responsibilities with respect to the use of government owned or leased computers. During the initial boot of a computer-based system and before any user can perform any work, a warning message must appear on the CRT screen in a fashion that requires the user to take an overt action to clear the screen. That is, the

message must not automatically scroll off the screen. The user must at least strike a key to clear the message from the screen. Appendix D contains the required text of the warning message. The appendix also contains instructions for loading a Warning Banner to MS-DOS based systems. Warning screen banners are also required to appear on terminals connected to MCDN or like networks.

b. Copyright Restrictions Copyright laws (Public Law 102-561 Copyright Infringement) must not be violated. Do not accept copied or pirated software. Personnel must be aware of copyright restrictions placed on the use of computer software by the authorized vendor. Additionally,

unauthorized copies of software may contain unknown code that inflicts a virus that may destroy or contaminate the computer-based system.

2.3.14. Computer Security Reporting ProceduresThe following guidance is provided for reporting actual or suspected computer security violations, (i.e. compromise of systems or data as a result of espionage, sabotage, fraud, misappropriation, misuse) and viruses:

- a. Marine Corps personnel will immediately report through their organizational chain any indication of computer security violations or viruses to the computer systems security officer or the security manager for the local command.

- b. Commands will report by naval message ~~or~~ e-Mail within 24 hours to CMC (Code CSBT) any occurrence where preliminary investigations confirm a possible security violation or virus attack. The message must include a point of contact with knowledge of the violation being reported.

- c. Local commands should determine if Naval Criminal Investigative Service (NCIS) involvement in computer security violations is warranted. CMC (Code CSBT) will notify Naval Electronics Systems Security Engineering Center (NAVELEXSECCEN) if their services are required to support a computer virus problem reported by a command.

- d. Dialogue between CMC and the field command will continue until the reported computer security issue is considered under control or resolved.

- e. Additional information and guidance pertaining to viruses are contained in IRM-5239-10, "SMALL COMPUTER SYSTEMS SECURITY."

Chapter Table of Contents

Chapter 3

PERSONNEL SECURITY

Paragraph Page

Section 1. <u>INFORMATION</u>	3.1. 3-3
Section 2. <u>SENSITIVE DUTIES</u>	3.2. 3-3
Section 3. <u>BACKGROUND INVESTIGATION</u>	3.3. 3-4
Section 4. <u>SECURITY BRIEFING</u>	3.4. 3-4
Section 5. <u>SECURITY DEBRIEFING</u>	3.5. 3-5
Section 6. <u>DECLINATION</u>	3.6. 3-5
Section 7. <u>PERSONNEL AWARENESS</u>	3.7. 3-5

(This page intentionally left blank)

CHAPTER 3

PERSONNEL SECURITY

3.1. INFORMATION Marine Corps computer facilities present a protection spectrum, ranging from relatively simple unclassified batch processing applications through more complex on-line systems where the protection of individual privacy and safeguards against criminal misuse are obligatory, to classified systems which support the Command Elements, Fleet Marine Forces or special operations.

a. Trained personnel are among the computer facility manager's most critical resources. In particular, leadership and supervision constitute the greatest challenge. Without skilled, loyal, motivated individuals, the most advanced technological computer hardware and software would be diminished in achieving organizational goals and successfully accomplishing the mission.

b. It has long been routine to require personnel associated with data processing functions to have security clearances appropriate to the highest level of the classified data processed. However, little consideration has been given to ensuring the continuing reliability of such personnel once their background investigations were favorably completed. For this reason, a continuous, positive, facility management effort is necessary to ensure the continued loyalty and reliability of individuals assigned to sensitive duties.

3.2. SENSITIVE DUTIES. The personnel function is the key ingredient to a successful computer security program. Personnel security measures are directly related to establishing the proper organizational framework for effective security, developing effective assignment and hiring practices, and maintaining positive employee relationships. As previously stated, people represent an organization's greatest asset, but from a security standpoint also pose the greatest threat. Basic policy governing the administration of personnel security investigations, security clearances and access is contained in OPNAVINST 5510.1H. Instructions for Marine Corps implementation are contained in MCO 5521.3H.

a. The individual computer facility manager is most familiar with the security environment of the daily operation, the threats to it, and the strengths and weaknesses of personnel. As such, he/she is most qualified to determine individuals best suited for specific billet assignments and to identify and remove from sensitive duties those personnel representing a risk to the facility or the data and assets contained therein.

b. Computer facility managers will ensure that sensitive positions under their jurisdiction are formally identified and designated as sensitive. For all computer facilities (design and operation) assigned the responsibility of processing Classified data or Sensitive Unclassified data, the following positions (as a minimum) will be designated as sensitive:

(1) Facility director.

(2) CSSO.

(3) System programmers.

(4) Computer operators.

(5) System analyst/Functional manager liaison.

c. In addition to the above positions, other positions may be designated sensitive depending on their purpose and function to the organization. An application programmer position, for example, is not necessarily a sensitive position. However, if the incumbent is involved with programs which process classified data, privacy data, financial data, etc., or has access to such programs, then the position should be designated sensitive. As the level of sensitivity decreases, it can be expected that the percentage of positions designated sensitive should also decrease.

3.3. BACKGROUND INVESTIGATION All personnel, whether military or civilian, will be subjected to a National Agency Check (NAC) as a part of their entry screening.

a. A favorable NAC and a satisfactory review of an individual's service or employment record, including an acceptable performance record, should provide the local commander a basis for authorizing a responsible individual access not only to Sensitive Unclassified information (if the duties so require), but also classified information at the SECRET level. ADP installation managers may utilize the NAC plus the initial screening and evaluation interview as a basis for the granting of Interim SECRET clearances. This will allow personnel to access computer systems engaged in the processing of general business applications classified no higher than SECRET.

b. Computer systems which process or store TOP SECRET data will be accessed only by persons holding TOP SECRET clearances resulting from the conduct of a favorable Background Investigation (BI). TOP SECRET systems containing SCI or SIOP-ESI data require a SBI of all personnel exposed to their classified data.

3.4. SECURITY BRIEFING All computer personnel will be given a security briefing upon arrival and prior to beginning their assigned duties. The briefing may be given by the manager or delegated to the CSSO. It will be tailored to the assigned duties and oriented toward the local security environment and include the computer hardware, software and data sensitivity level.

a. The briefing will stress the importance of the individual's duties as a part of the unit mission and emphasize individual security responsibilities. No question having security impact will be allowed to go unanswered and no person will begin duties in a classified and/or sensitive area without a clear understanding of what is expected. The appropriate personnel available for questions throughout the assignment will be identified.

3.5. SECURITY DEBRIEFING Upon termination of employment in sensitive computer duties or temporary separation for a 60-day period or more, military members, civilian employees, foreign nationals, and contractor personnel will be debriefed, will return all material related to the computer facility, and will be required to execute a security termination statement.

a. The statement will include an acknowledgment that the individual has accomplished the following:

(1) Has read the appropriate provisions of the Espionage Laws (Appendix F of OPNAVINST 5510.1H), other federal and criminal statutes, and local regulations applicable to the level of classified and/or Sensitive Unclassified information to which the individual had been granted access.

(2) No longer possesses or has access to any proprietary or Sensitive Unclassified information.

(3) Will not communicate or transmit classified or Sensitive Unclassified information to any unauthorized person or source.

(4) Will report without delay to the FBI or the Marine Corps security office, as appropriate, any unauthorized attempt to solicit classified or Sensitive Unclassified information.

3.6. DECLINATION. Should an individual refuse to execute a debriefing statement, that information will be reported immediately to the security office of the computer facility or organization concerned followed by an entry in the security log for future reference or reporting.

3.7. PERSONNEL AWARENESS Measures must be taken to ensure the security of data and information from disgruntled employees. Formal procedures must be identified and implemented for most situations that are vital to an organization. These situations do not necessarily have to be sensitive or critical in nature. Another related matter that must be addressed is the potential for system sabotage by employees. There are certain signs to look for in employees that have recently been reassigned or removed from a section because of poor performance or relations. Anger, bitterness, vindictiveness, or threats and revenge promises should not be taken lightly when the employee has access to a terminal or a computer. Immediate action must be taken to safeguard information and data. Anticipating a problem and taking measures before the employee is actually fired or removed can ensure system integrity.

Chapter Table of Contents

Chapter 4

PHYSICAL SECURITY

Paragraph Page

Section 1. <u>INFORMATION</u>	4.1. 4-3
Section 2. <u>PHYSICAL SECURITY PRINCIPLES</u>	4.2. 4-3
Evaluate Requirements	4.2.1. 4-3
Section 3. <u>SECURITY OF REMOTE DEVICES</u>	4.3. 4-4
Remote Terminal Area Security	4.3.1. 4-4
Access Controls	4.3.2. 4-4
Acoustic Coupling	4.3.3. 4-4
Section 4. <u>SECURITY REVIEWS</u>	4.4. 4-4
Section 5. <u>EFFECTS OF MAGNETISM</u>	4.5. 4-5

(This page intentionally left blank)

Chapter 4

PHYSICAL SECURITY

4.1. INFORMATION A balanced computer security program must include a firm physical security foundation. The objectives are to safeguard personnel, prevent unauthorized access to assets (i.e., facility, equipment, material, documents), safeguard against espionage, sabotage, damage, theft, and reduce the exposure to threats which could result in a disruption or denial of service.

4.2. PHYSICAL SECURITY PRINCIPLES The diversity of computer facilities within the Marine Corps makes it undesirable to establish universal, rigid physical security standards. However, it is recognized that adequate physical security at each facility is important to achieving a secure processing environment.

4.2.1. Evaluate Requirements Physical security standards must be based on an analysis of mission criticality, sensitivity levels of the information processed, overall value of the information, local criminal and intelligence threat, and the value of the computer systems/peripheral equipment. This will be achieved through adherence to the basic principles stated below:

- a. Physical security is provided through an in-depth application of barriers and procedures, including continual surveillance (human or electronic) of the protected area. Barriers and procedures include structural standards, key control, lighting, lock application, and inventory and accountability.
- b. Physical access controls, commensurate with the level of processing, will be established to deter unauthorized entry into the computer facility and other critical areas which support or affect the overall operation.
- c. Physical access to sensitive media files or libraries will be restricted to individuals assigned that responsibility. Magnetic media and supporting documentation used to process classified information or other National Defense requirements will be secured in accordance with applicable regulations.
- d. The effects of disasters such as fire and floods will be prevented, controlled, or minimized to

the extent economically feasible by the use of detection equipment, fire extinguishing systems, and tested emergency measures.

e. Facilities selected or designed to house computer equipment will be of sufficient structural integrity to provide, or will be capable of being made to provide, effective physical security at a reasonable cost.

4.3. SECURITY OF REMOTE DEVICES The introduction and use of large-scale, remotely accessed computer systems and networks require that all terminal connecting equipment be protected according to the data sensitivity level to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification. Additionally, MCO P5510.14 requires any organization that is connected by a remote terminal device to a main or host computer be responsible for the appointment of a Terminal Area Security Officer (TASO).

4.3.1. Remote Terminal Area Security Remote terminal devices must be secured during and after normal operational hours consistent with the mode of operation and level of information which the remote terminal is authorized to access.

4.3.2. Access Controls Safeguards will be implemented to ensure that only authorized persons use remote terminal equipment capable of accessing sensitive computer systems. Caution will also be used to ensure that sensitive hard copy output is received and removed from the terminal area only by authorized persons. After normal business hours or during periods when effective monitoring cannot be maintained, all physical access to the area will be secured. Remote terminals will be disabled from the system at the host or remote concentrator during non-duty hours. If this disabling is via a logical disconnect, then a periodic check should be made by the system to verify that the disconnect is still valid. For information and guidance concerning access to Marine Corps systems connected by the Marine Corps Data Network (MCDN), refer to IRM-5239-06, "DATA ACCESS SECURITY."

4.3.3. Acoustic Coupling Because of the increased vulnerability inherent in acoustically-coupled terminals, their use in accessing sensitive systems should be minimized and where practical prohibited (non-acoustically coupled devices are currently considered the industry standard). If such devices are used to access commercial time-sharing services, they should be located in an area that can be secured after normal business hours. If this is not possible, other measures such as use of a telephone lock or removal of the acoustic coupler should be considered.

4.4. SECURITY REVIEWS Physical security reviews of computer facilities and supporting areas

designated to process sensitive information will be conducted annually as part of the facility risk management program. Specific items for consideration should include adequacy of physical barriers, access and egress controls, and the use of guard personnel from the first barrier (wall) surrounding the computer system outward. The review will also provide an assessment of the overall posture, such as breaches of physical security, bomb threats, fire, and natural disasters. Physical security inspectors will not inspect internal operating procedures and computer system security. For further information and guidance concerning physical security, refer to OPNAVINST 5530.14, DON Physical Security and Loss Prevention Manual.

4.5. EFFECTS OF MAGNETISM While magnetic hazards to storage media have received attention beyond the real potential danger, possible damage from this source cannot be discounted. In this regard, attention should be given to the effect upon magnetic media placed in proximity to circuits that could serve as electrical conductors.

Chapter Table of Contents

Chapter 5

HARDWARE SECURITY

Paragraph Page

Section 1. <u>IMPORTANCE OF HARDWARE SECURITY</u>	5.1. 5-3
Section 2. <u>SUPPORT FOR TRUSTED SYSTEMS</u>	5.2. 5-3
Hardware Architecture	5.2.1. 5-3
Section 3. <u>SPECIAL CONSIDERATIONS</u>	5.3. 5-5
Hardware Maintenance	5.3.1. 5-5

(This page intentionally left blank)

Chapter 5

HARDWARE SECURITY

5.1. IMPORTANCE OF HARDWARE SECURITY Hardware resident architectural features are an important element in the enhancement of total automated system security. Depending on the age, sophistication, and design of the computer system, hardware based security controls are an important factor when evaluating the security environment of any system. The absence of hardware security features or the presence of known hardware vulnerabilities will require compensation in other elements of the computer security program.

5.2. SUPPORT FOR TRUSTED SYSTEMS Significant research and development are underway to design trusted computer hardware and software system components. A trusted system employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of classified or Sensitive Unclassified information. Consequently, it is the intent of this chapter to provide basic general guidance in this field, and to suggest that hardware and software security requirements be considered in future design, development, and acquisition of systems equipment. Memory and storage protection, implemented through hardware controls and supplemented by system software, should be exercised by the system over the memory addresses to which a user program has access. DOD 5200.28-STD requires that all computer resources that process or handle classified or Sensitive Unclassified information shall implement as a minimum Class C2 functionality (controlled access protection). Desirable hardware architectural features are discussed in the next paragraph.

5.2.1. Hardware Architecture Hardware architectural features include, but are not limited to, the following:

- a. The operational state of a processor should include one or more protection variables. These variables determine how the processor interprets instructions. For example, a processor might have a master and user mode protection state variable in which certain instructions are illegal except in master mode. Modification of the protection state variable must be prevented by the operating system and hardware to prevent unauthorized access.

- b. The ability of a processor to access locations in memory (including primary and auxiliary memory) must be controlled. For example, in user mode, a memory access control register might allow access to only memory locations allocated to the user.

- c. Certain instructions should depend on the protection state of the processor. For example, instructions which perform input or output operations would execute only when in the master mode. Any attempt to execute an instruction which is not authorized should result in a hardware interrupt which will permit the operating system to interrupt or abort the program containing the illegal instruction.
- d. All possible operation codes, with all possible tags or modifiers, whether legal or not, should produce known responses.
- e. All registers should be able to protect their contents by error detection or redundancy checks which set protection state variables, control input or output operations, execute instructions, or which are otherwise fundamental to the secure operation of the hardware.
- f. The contents of any register which can be loaded by the operating system should be storable. This would permit the operating system to check its current value against its presumed value. The term "register" as used here and in the above refers primarily to index or general-purpose registers, rather than an isolated address or a single storage location within the computer.
- g. Error detection should be performed on each fetch cycle of an instruction and its operand (such as parity check and address bounds check). Equipment controls and integrity features, such as parity characters and validity checks, enhance system security and provide protection against equipment malfunction.
- h. Error detection (such as parity checks) and memory bounds checking should be performed on transfers of data between memory and storage devices or terminals.
- i. Automatic, programmed interrupts should control system malfunction and detect operator error.
- j. Read, write, and execute access rights of the user should be verified.
- k. Hardware should have the capability to isolate users from each other, the protection control mechanisms of the operating system, and the operating system. The principal hardware controls that isolate users are base-addressing registers, bounds registers, and checking circuits which

make sure that programmed memory addresses limit access to specific, authorized programs and data.

1. Certain hardware measures can be used in remotely accessed computer systems to improve means to authenticate users and terminal devices. These include the use of hardware-generated or firmware-generated characters that identify the terminal to the central system when connected, or magnetically encoded badges or cards which activate the terminal device when inserted into a reader.

5.3. SPECIAL CONSIDERATIONS Special consideration is required for systems that process classified data. Removable storage media used for classified processing will be protected as classified. Storage media containing Sensitive Unclassified information must be protected to ensure against unauthorized access. Consideration must also be given to the availability of a cleared repair facility to ensure continued protection of any residual classified data.

5.3.1. Hardware Maintenance A system maintenance concept must be included in the total hardware protection environment. Special consideration should be given to maintenance of small computers used to process classified information. Several factors to consider in developing a maintenance concept follow:

a. Systems must be properly maintained to ensure availability and integrity. The user is responsible for making sure preventive, emergency, and remedial maintenance is performed as required by the owner's manual and contract.

b. System users must be trained to operate the system to avoid serious maintenance problems (e.g., incorrect loading and unloading of disks or tapes, powering system on and off, etc.). Vendor operating instructions should be reviewed and applied.

c. The maintenance concept should be responsive to operational requirements. Particular emphasis should be placed on maintenance required for locations outside the continental United States (CONUS) and in deployment situations.

d. Equipment maintenance must be restricted to authorized or identified vendor maintenance personnel. Operator and user maintenance must be restricted to normal cleaning and housekeeping activities to make sure equipment is operated and maintained to protect Marine

Corps rights under warranties.

e. Classified media, products etc, must not be given to vendor maintenance personnel for testing or use.

f. Vendor personnel who must enter areas where classified information is processed must have the proper security clearance or be constantly escorted until all maintenance is completed. Escorts must be briefed by the CSSO on their responsibilities while performing escort duties. ~~un~~cleared maintenance personnel.

g. The impact of dial-in diagnostics and maintenance must be evaluated as an integral part of the security plan.

Chapter Table of Contents

Chapter 6

SOFTWARE SECURITY

Paragraph Page

Section 1. <u>GENERAL REQUIREMENTS</u>	6.1. 6-3
Class C2 Protection	6.1.1. 6-3
Minimal Protection	6.1.2. 6-3
Section 2. <u>TYPES OF SOFTWARE</u>	6.2. 6-3
Security Requirements	6.2.1. 6-3
General Purpose Software	6.2.2. 6-3
Applications Software	6.2.3. 6-4
Section 3. <u>ACCESS CONTROLS</u>	6.3. 6-4
Identification And Authorization	6.3.1. 6-4
Audit Trails	6.3.2. 6-4
File Protection And Control	6.3.3. 6-5
Minimum Requirements	6.3.4. 6-6
Section 4. <u>SOFTWARE DEVELOPMENT</u>	6.4. 6-7

Quality Control	6.4.1. 6-8
Life-Cycle Process.....	6.4.2. 6-8
Configuration Management	6.4.3. 6-8
High-Order Languages (HOL)	6.4.4. 6-9
Documentation	6.4.5. 6-9
Testing	6.4.6. 6-9
Minimum Requirements	6.4.7. 6-9
Section 5. <u>DATA BASE MANAGEMENT SYSTEM(DBMS)</u>	6.5. 6-10
Section 6. <u>UTILITY SOFTWARE</u>	6.6. 6-10
Section 7. <u>LEAST PRIVILEGE</u>	6.7. 6-10
<u>Paragraph Page</u>	
Section 8. <u>TRUSTED COMPUTER SYSTEMS</u>	6.8. 6-10
Software Security Packages	6.8.1. 6-11
Section 9. <u>SOFTWARE CERTIFICATION</u>	6.9. 6-11
Concept	6.9.1. 6-11
Minimum Requirements	6.9.2. 6-11

(This page intentionally left blank)

Chapter 6

SOFTWARE SECURITY

6.1. GENERAL REQUIREMENTS This chapter applies to all software used on Marine Corps computers regardless of how it is acquired. It prescribes the amount of protection to be provided by and for the software. These requirements apply to Marine Corps and contractor developed software. Where feasible, changes should be made to previously developed software to enable it to meet the prescribed security requirements for classified or Sensitive Unclassified processing as defined in DoD 5200.28-STD and documented as an integral element of security life cycle management. The DoD Directive 5200.28 requires all computer resources that process or handle Classified or Sensitive Unclassified information to implement at least Class C2 functionality (Controlled Access Protection). If these Class C2 requirements cannot be met (including manual alternatives), they should be documented in the risk assessment.

6.1.1. Class C2 Protection Class C2 protection provides for discretionary access control, memory clearing before reuse, identification and authentication and audit trails. Implementation of Class C2 security for all appropriate systems may not be feasible if the required security technology is not available. Responsible organizations may request waivers to MCCDC (AS) of this requirement under those conditions.

6.1.2. Minimal Protection Personal computers (Micro's) will be protected by hardware, software and security operating procedures to provide reasonable security until such time as effective Class C2 protection becomes available for personal computers.

6.2. TYPES OF SOFTWARE Software-based protective controls complement and support hardware protective features of computer circuitry. Increasing reliance on software-based computer security will require safeguards within executive, utility, and applications software. Vendor security software products are becoming readily available and offer a wide variety of security features and degrees of software protection.

6.2.1. Security Requirements Responsible individuals tasked with conducting pre-procurement reviews of software requirements will consider the adequacy of software security controls and ensure that procurement documents include security requirements appropriate for the sensitivity level of the system. Types of software are identified below.

6.2.2. General Purpose Software This type includes the following:

a. Executive software controlling the operation of the computer equipment (i.e., the operating system, supervisors, software input/output controllers, and accounting systems embedded in or complementing the operating system).

b. Utility software supporting executive and applications software (i.e., sort/merge routines, data management systems, interpreters, and converters).

c. Software tools used in the development of applications software.

6.2.3. Applications Software This type of software includes routines and programs designed by or for, system users and customers. Applications software is functionally oriented, problem-solving software. By using available automated system equipment and general purpose software, applications software completes specific, mission-oriented tasks, jobs, or functions. Except for general purpose packages acquired directly from software vendors or from the original equipment manufacturers, this type of software is generally developed by the user with in-house resources or through contract support.

6.3. ACCESS CONTROLS Software security is the last line of defense to detect and prevent unauthorized access. Most reported computer offenses are committed by users with authorized access to the system. The following provides methods for obtaining the required degree of protection.

6.3.1. Identification And Authorization Passwords are the most popular form of access control. They are inexpensive, completely software supportable, and relatively painless to use. They are also a source of system vulnerabilities if not implemented securely and maintained. Too many users tend to believe that passwords are intuitively secure. Unfortunately, this is not the case. Improper password protection allows the improper use of properly granted rights by a subverted agent whose actions cannot be directly observed. The primary vulnerability of passwords is that the user must memorize a sequence of characters. The sequence must be random; however, the password may be pronounceable by randomly concatenating words or syllables. The user-ID should be unique so that when a user-ID is locked out by exceeding the number of allowable access attempts it will only affect one user. User-ID's are an unclassified reference to a user that can be displayed on printouts and audit trails without compromising the passwords. For additional information concerning standardized use of passwords and user-ID's, refer to IRM-5239-06, "DATA ACCESS SECURITY."

6.3.2. Audit Trails An audit trail allows the CSSO to monitor activities on the system, and reminds users that their actions are subject to monitoring. Some audit trails only record successful and unsuccessful access attempts; however, to be a more effective security tool, an audit trail must track all events including file accesses, type of transaction, peripheral usage, password changes and locking a user-ID because the password has expired.

a. The audit trail must also track use of privileged, supervisory, or system level commands or instructions that can circumvent established security controls.

b. Passwords should not be recorded in the audit trail so the audit trail can remain unclassified. This includes character strings incorrectly given as passwords possibly exposing a password. An audit trail should inform the user, during system log-in, of the date, time, and location of the last time the user-ID was used. This could help detect a compromised password.

c. If manual audit trails are used, the CSSO should make random checks to make sure users are recording system usage. Audit trail files must be protected to prevent unauthorized changes or destruction. As a minimum, the file should be protected so only the CSSO can make changes or delete the file.

6.3.3. File Protection And Control Files are logical groupings of data and programs stored within a system allowing each user to access portions of the information stored. In system high, controlled, or multilevel security modes, files should be given another level of protection like data encryption to prevent compromise and to enforce need-to-know requirements. For critical systems, file backup and recovery are essential.

a. Permissions Access to a file should be regulated by using permissions. A permission describes transactions allowed on a file not owned by the user. Possible permissions include read, write, execute, add, delete, and modify.

b. Backup and Recovery Two of the most important safeguards for critical systems are backup and recovery. Backup is a duplicate copy of a file that is maintained separately from the system and used if the original copy is lost or destroyed. Recovery is the process of reconstructing a file based upon a record of all file transactions since the last backup. All systems should have backup procedures, but not all systems will require recovery capabilities. A recovery capability can be expensive in system time and storage. To determine the proper length of time between backups and the need for a recovery capability, consider the following:

- (1) Criticality of the system and files.
- (2) How much and how often the files change.
- (3) Cost of backup or recovery software.
- (4) Manpower cost to perform backup.
- (5) Capability of duplicating lost information.
- (6) Cost of reentering lost information.
- (7) Effect on mission if information is not replaced.

c. Encryption File encryption is another method to protect files. Using encryption requires more time to store and load files, but it is effective. For a number of years, the Government has endorsed a publicly published (FIPS PUB 46-1) cryptographic algorithm (i.e., a technical explanation of one way to accomplish encryption and decrypting) called the Data Encryption

Standard (DES). A related U.S. Government standard - known as Federal Standard 1027 - provides technical standards for how the DES algorithm should be built into cryptographic hardware. Cryptographic products that are endorsed by the National Security Agency as meeting Federal Standard 1027 are contained on the NSA Endorsed Data Encryption Standard (DES) Products List. These DES products have been endorsed for use in protecting U.S. Government or U.S. Government-derived Sensitive Unclassified information during transmission. They not be used to secure classified information.

6.3.4. Minimum Requirements Minimum requirements for access controls are listed below. Some pertain to classified systems only. If any of the automated requirements are not possible or available for a system, an equivalent manual method may be substituted. If the manual method is not possible, document that fact in the risk assessment. Deviations from the following minimum

requirements may be necessary to accommodate conditions that vary from one computer facility to another. Conditions to consider include: the physical environment, volume, frequency, sensitivity, and criticality of processing; mode of operation; system configuration; and hardware and software functional capabilities.

a. All classified and Sensitive Unclassified multiuser systems must have some form of system access control. The most common type is the use of a password.

b. Passwords must contain at least seven characters but may be longer. Maximum lifetime of a password cannot exceed one year.

c. If automated, the password system should verify that only characters in the selected subset have been generated or selected when a password is created or changed. It must also verify that the passwords are an acceptable length.

d. The selected password length range must provide a level of protection commensurate to the value or sensitivity of the resources or data it protects.

e. Classified users should sign for the original password verifying they understand the requirements for protecting the password.

f. A single point of contact with one alternate should manage and control passwords. Additional control points may be used for systems with geographically separated remote processing sites for networks.

g. Personal passwords must be distributed from the password source so only the user has access to the password.

h. A password must be changed as quickly as possible but at least within 1 workday of a possible compromise or mishandling of the password.

i. A password must be suspended immediately when the user leaves the organization. If the

individual uses a group password, the group password will be changed immediately.

j. A password must be deleted when the user no longer requires the access for a period greater than 90 days. This includes temporary duty travel and permanent or temporary reorganization transfer.

k. Users who create or select their own password must be instructed to use a password selected at random, and never one related to their personal identity, history or environment.

l. Critical files will be routinely backed up. The periods between backup should depend on system criticality and frequency of changes.

m. Purchased software should be backed up within the limits set by copyright laws and the purchase agreement. Official DOD generated software must be backed up or methods identified to obtain a copy.

n. For applications critically dependent on the proper operation of the software, a backup copy of the software should be routinely compiled and compared to the working copy to detect unauthorized alterations.

o. Software developed or purchased to handle Sensitive Unclassified data (refer to Appendix E), must have configuration management controls to protect against unauthorized alteration. If the software is contained on removable magnetic media, a

magnetic media label (sticker) must be placed on the media for identification and protection as required by law. The label reads "This medium is SENSITIVE UNCLASSIFIED U.S. Government Property. Protect it from unauthorized disclosure." Sensitive Unclassified labels (NAVMC 11196) for removable media are available through the Marine Corps supply system and are listed in Appendix C.

6.4. SOFTWARE DEVELOPMENT Although most access control mechanisms are in the operating system or special security package, security must be included in all levels of software. Software should be checked to make sure it does not circumvent system security controls. The level of security controls depends on the sensitivity and criticality of the system. Additional

controls can be implemented by application software to provide more detailed control than that built into the operating system.

6.4.1. Quality Control Quality control is a serious security concern since faulty software can produce undetected, inaccurate output that can affect the mission, or it can fail, causing denial of service. In most manual operations there are numerous quality control activities where unusual results are questioned and checks are used to detect errors. This capability must be included in the software to make the automated method as secure and reliable as the manual method. Below are some techniques to include in applications software to improve reliability:

- a. Edit input to agree with all assumptions made in the software and specifications.
- b. Perform range and reasonability checks throughout the software to ensure proper operation.
- c. Perform range and reasonability checks of the output to make sure it agrees with specifications.
- d. Provide additional checks before a critical code that can negatively affect the system, such as division by zero or memory accesses outside of the program area.
- e. Ensure edits default to error conditions rather than success.

6.4.2. Life-Cycle Process The life-cycle process of a system and its software are addressed in MCO P5231.1 and require that computer security elements be addressed explicitly in each Life-Cycle Management (LCM) phase. This is critical at the conceptual and design phases. Security added after these phases is often ineffective and more expensive.

6.4.3. Configuration Management While proper configuration management is important for all software, it is even more important when proper operation of the software is critical to the mission. Control of changes to software prevents faulty software or covert code from entering the system. Covert code may be in one of several forms called computer virus, trap door, Trojan horse, or a software time bomb. Following are suggestions to enhance configuration management:

- a. An office other than the development office should control changes, from the initial change request to implementation.
- b. Changes should not be implemented by the office coding the changes.
- c. Changes should be examined at several levels within the development organization to make sure only authorized code is included. These examinations should be documented.
- d. After verification at all levels, changes should be applied to a protected source. Testing before verification should be performed on a copy of the software.
- e. After changes are applied, new software should be compared to the working copy used for testing to make sure only authorized changes were made and test results are valid.
- f. A new, protected source copy should be made and stored away from the system. The original is then the new working copy for operation or further developments and changes.

6.4.4. High-Order Languages (HOL) Standard use of HOL improves security. HOL restricts programmers from circumventing existing controls provided by the operating system such as not allowing memory access outside of the allotted program space. In addition, programs using HOL

are usually less complicated and are thus easier to maintain and less likely to contain errors that could harm the system. It is also harder to hide covert code in a program written in a HOL.

6.4.5. Documentation End-product documentation for the user, operator, and programmer should include an explanation of software security features so they can be used effectively and not circumvented or destroyed by improper usage or by a change made to the program. User documentation should contain detailed information concerning software use. Programmer documentation should contain a description of the internal software operation. This information could be classified or Sensitive Unclassified and could make the software vulnerable to improper use or change. Documentation must be protected or controlled commensurate with the classification or usefulness of the information it contains and placed under configuration management control.

6.4.6. Testing Security included in the design of software must be tested to make sure it operates properly. Testing must be thorough since security controls must also protect against intentional hostile acts as well as accidents.

6.4.7. Minimum Requirements Requirements stated below should be used whether software is developed by the Marine Corps or by a contractor. Purchased commercial off-the-shelf software should be selected using these criteria. Requirements that cannot be satisfied due to cost or nonavailability should be carefully evaluated and documented in the risk assessment process. Commercial off-the-shelf software should also be tested by a competent organization and certified by the DAA if it contains security controls. All public domain software should be tested by a competent organization and certified by the DAA to be free of any known security problems before being used.

a. Unless justifiably approved by the DAA, no application software may circumvent the security provided by the operating system or special security software.

b. A security requirement statement must be part of the requirements documents for software on sensitive or critical systems. This statement should be based on a preliminary sensitivity and criticality analysis and must describe security software requirements needed to adequately protect the system and the information it processes.

c. Software documentation must include a description of the security provided by the system and what is required of the user, operator, or programmer.

6.5. DATA BASE MANAGEMENT SYSTEM (DBMS) Data bases with a DBMS should be given additional protection because of increased ease of obtaining correlated data. A DBMS combines information and provides tools for correlating the information to obtain additional information through aggregation. Because new information may be of a higher sensitivity than the original, it may be necessary to protect the entire data base at a higher level than individual data elements of the data base. During the threat and vulnerability analysis of the risk assessment, systems with a DBMS could have a slightly higher threat identified. The DBMS should provide file control and protection (paragraph 6.3). The DBMS must not circumvent the controls present on the system.

6.6. UTILITY SOFTWARE Only specifically identified personnel authorized by management are

allowed access to system utilities provided by the operating system software or other add-on software. These utilities are usually very powerful and have fewer checks to prevent erroneous inputs. Sometimes the system will limit the scope of these utilities to prevent users from affecting other users. For example, a deletion utility should allow users to delete only their own files.

6.7. LEAST PRIVILEGE Systems software and applications software shall function so that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but to no more. In the case of "need to know" for classified information, access must be essential for accomplishment of lawful and authorized Government purposes.

6.8. TRUSTED COMPUTER SYSTEMS Special expertise must be used in designing and testing software for it to make critical decisions involving the protection of classified or Sensitive Unclassified information. Software that has been given this special attention is termed trusted software. Trusted software, regardless of how developed, must only be tested by an authorized agency. Trusted software must be evaluated by standards found in the DOD Standard 5200.28-STD. Formally evaluated software will receive a rating of the level of protection it provides. This rating can then be used to determine if the software is suitable for a particular security processing mode. Minimum ratings for each security mode are listed and described in Appendix F, "Security Modes of Operation." The National Computer Security Center (NCSC) publishes an Evaluated Products List (EPL) which includes the security functions of the products evaluated and their assigned ratings.

6.8.1. Software Security Packages To provide operating systems with enough security to be considered trusted, an increasing number of vendors are providing system and subsystem software security packages which attach to the system and provide many of the capabilities of a trusted system. Vendors submit their products to the NCSC for evaluation. These packages may significantly improve the security of a system and should be seriously considered. Review the NSA Evaluated Products List to determine available products and their associated ratings.

6.9. SOFTWARE CERTIFICATION Software for mission critical systems must have a method of providing quality assurance, called certification.

6.9.1. Concept. Before certification, software and related documentation must be tested to make sure it provides the quality assurance and security controls required. This is part of the Security Test and Evaluation (ST&E). Security controls and software must be tested to make sure they do not circumvent any security controls already in the system. ST&E should be performed by an organization other than the developing organization. Commercial off-the-shelf and public

domain software also should be tested and certified if it contains security controls. A software release or version need only be certified once and a copy of the certification letter included with all copies of the software.

6.9.2. Minimum RequirementsThe requirements stated below apply to all software.

- a. Software trusted to make decisions involving classified information must be evaluated to meet the criteria of DOD Standard 5200.28-STD.
- b. To prevent unauthorized modification, software providing internal security controls which identify and separate users and data must be protected commensurate with the highest sensitivity level of the information processed.
- c. Marine Corps developed software containing security controls, including new releases for use on sensitive or critical systems, must be certified by the responsible manager of the developing activity.
- d. Contractor developed software containing security controls for use on mission critical systems must be initially certified by the senior manager of the organization responsible for the acquisition.
- e. 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.
- f. Use only official U.S. Government authorized bulletin boards. It is imperative that the software/information from a bulletin board be tested for the presence of a virus by the individual or organization responsible for computer security matters. (Ensure that software/information 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 U.S. Government sanctioned bulletin board and has been tested for the presence of a virus before it is used.
- g. Privately owned commercial software and game software is not authorized. Only U.S. Government software developed and approved or commercial software procured through the

supply system are authorized.

Chapter Table of Contents

Chapter 7

COMMUNICATIONS SECURITY (COMSEC)

Paragraph Page

Section 1. <u>INFORMATION</u>	7.1. 7-3
Section 2. <u>PROVISIONS OF ENCRYPTION EQUIPMENT</u>	7.2. 7-3
Security Systems And Methods	7.2.1. 7-3
Terminal Access	7.2.2. 7-3
System Password Control	7.2.3. 7-4
Section 3. <u>PROTECTION FROM IMPROVISED COMSEC</u>	7.3. 7-4
Section 4. <u>COMSEC PLANNING</u>	7.4. 7-4

(This page intentionally left blank)

Chapter 7

COMMUNICATIONS SECURITY (COMSEC)

7.1. INFORMATION Communications Security (COMSEC) policy requires that all record telecommunications be separated into two categories: classified and unclassified communications. All communications circuits employed to interconnect remotely located components of Marine Corps automated systems or networks which process classified or Sensitive Unclassified information will be provided COMSEC. Appropriate COMSEC will be achieved by use of standard military encryption systems produced and or endorsed by the National Security Agency (NSA), installed in accordance with the provisions of NACSIM 2203; Protected Distribution System (PDS) or intrusion-resistant cables. PDS wiring/cable will be installed as prescribed by NACSIM 2203. A PDS is costly and suitable for only short-distance communication (normally within a single building or facility, which is under continuous physical/personnel security controls), and approved methods of user-authentication.

7.2. PROVISION OF ENCRYPTION EQUIPMENT Telecommunications circuits of Marine Corps automation systems handling classified information will be encrypted using only NSA endorsed Type I COMSEC equipment. Telecommunications circuits handling Sensitive Unclassified information may be encrypted using either NSA endorsed Type I or Type II equipments. Where operationally feasible, and cost effective, a PDS may provide the requisite security, as an alternative to encryption. All COMSEC equipment is procured for the Department of the Navy by the Chief of Naval Operations. Unless specifically authorized by CMC, Marine Corps commands are not authorized to procure COMSEC equipment. Requirements for COMSEC equipment will be identified to CMC (CSBT), via the chain of command, for inclusion in the DON centrally funded COMSEC procurement program.

7.2.1. Security Systems And Methods Sensitive Unclassified information including privacy, financial, asset/resource, proprietary, or other Sensitive Unclassified information (including data aggregation) which automated systems are obligated to protect (to include the Computer Security Act of 1987), may be safeguarded against unauthorized use by installation of software/hardware log-on procedures commonly employed on remotely accessed, resource-shared systems. These procedures require each authorized user to authenticate oneself to the system. The same principle may be further developed, if deemed necessary, by applying unique passwords to protect individual files within a systems catalogue.

7.2.2. Terminal Access Most commercially available log-on software routines permit adjustment of the number of erroneous log-on attempts before the remote terminal device is "locked-out." Systems which permit more than a single log-on attempt before lockout are theoretically vulnerable to an infinite number of log-on attempts. Therefore, log-on attempts for classified

systems should be limited to two. For Sensitive Unclassified systems, the DAA may permit up to three log-on attempts.

a. Terminal devices which are locked out should be "unlocked" by operators of the host computer site only after such action has been authorized by the CSSO, or, if site procedures permit, upon request of the TASO responsible for the terminal on which the lockout occurred. At locations where personal contact between the TASO/CSSO and the host system is not possible, the "unlock" authorization may be passed by telephone (preferably using a STU-III telephone in the secure mode), provided an authorized authentication system is used to confirm the identity of the requestor. Authorized manual, paper-based voice authenticators and instruction on their use are available through the COMSEC Material System (CMS).

7.2.3. System Password Control All passwords are critical to the security of the system accessed and all associated activities. Persons using passwords employed on such systems must be instructed on password sensitivity, protection, and personal responsibility for their security. The potential value of system passwords to a hostile foreign nation far exceeds that normally assigned to safe combinations used to protect information of equivalent classification.

7.3. PROTECTION FROM IMPROVISED COMSEC Marine Corps automation facilities will use only COMSEC equipment and keying materials produced by the NSA and installed and secured in accordance with paragraph 7.1 when national defense information is passed over telecommunications circuits connecting remotely located peripheral or terminal devices with a host computer or among a group of host computers and their outstations which serve as components of a larger teleprocessing network.

a. The use of mathematical algorithms, compression, ~~or~~ compaction techniques, for the purpose of protecting classified information stored or processed with an automated system is prohibited. At no time will a Marine Corps automated system processing classified data attempt its protection during transmission over telecommunications circuits with commercially available computer-generated algorithm encryption systems such as the National Bureau of Standards Data Encryption Standard (DES).

7.4. COMSEC PLANNING System planners and engineers designing automated systems should consult with CMC (CSBT) during the early phases of their planning. Early coordination will aid in establishment of proper COMSEC requirements and ensure early inspection and technical guidance throughout the systems installation and testing. Refer to CMS-1 "Communications Security Material System (CMS) Policy and Procedures Manual".

Chapter Table of Contents

Chapter 8

EMANATIONS SECURITY (TEMPEST)

Paragraph Page

Section 1. <u>APPLICABILITY</u>	8.1. 8-3
Section 2. <u>INFORMATION</u>	8.2. 8-3
Section 3. <u>TEMPEST TERMINOLOGY</u>	8.3. 8-3
Section 4. <u>RESPONSIBILITIES & PROCEDURES</u>	8.4. 8-4
Section 5. <u>TEMPEST CONTROLS</u>	8.5. 8-4
Section 6. <u>FILTERED POWER</u>	8.6. 8-5
Section 7. <u>TEMPEST COUNTERMEASURES</u>	8.7. 8-5
Section 8. <u>PROTECTED DISTRIBUTION SYSTEM</u>	8.8. 8-5

(This page intentionally left blank)

Chapter 8

EMANATIONS SECURITY (TEMPEST)

8.1. APPLICABILITY. This chapter is applicable to only those computer facilities (any size) processing CLASSIFIED defense information. OPNAVINST C5510.93, "DON Implementation of National Policy on Control of Compromising Emanations (U)", promulgates DON implementation of national policy on control of compromising emanations, generally referred to as TEMPEST. It applies to all activities of the DON responsible for the design, procurement, installation, operation, maintenance, or repair of electronic equipment or systems used to process classified information.

8.2. INFORMATION. The presence of compromising emanations depends upon the type of equipment used to process the information; the method of installation; and the maintenance status of the equipment. NISE EAST carries out the compromising emanations (TEMPEST) control program for the Marine Corps. TEMPEST support takes three forms: instrumented TEMPEST tests, noninstrumented TEMPEST inspections, and technical advice and assistance. TEMPEST tests and inspections will be scheduled by NISE EAST as requested per submission of a TCR in accordance with OPNAVINST C5510.93. Supporting TEMPEST personnel should be contacted to obtain technical advice and assistance.

8.3. TEMPEST TERMINOLOGY

a. Compromising Emanations. These emanations are unintentional, intelligence bearing electromagnetic signals which might disclose sensitive information transmitted, received, handled or otherwise processed by an information processing system.

b. TEMPEST. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the "compromising emanations."

c. TEMPEST Countermeasure Review (TCR). Any system which is or will be used to process classified data (except those systems located on military bases within the U.S. that process data classified no higher than CONFIDENTIAL), must be afforded a TEMPEST Countermeasure Review. OPNAVINST C5510.93 details the information required to prepare and submit a TCR to NISE EAST. A TCR must be submitted (with the exception above) before a system or equipment can be used to process classified information. After the TCR has been submitted, classified

processing can begin on the system provided all the necessary countermeasures or procedures identified have been implemented.

8.4. RESPONSIBILITIES AND PROCEDURES The responsibilities of the Designated Approving Authority (DAA) is to accomplish the following:

- a. Ensure that the duties and responsibilities are fulfilled by Directors of computer facilities or organizations under their jurisdiction at both headquarters and subordinate levels.
- b. Ensure that TEMPEST technical assistance is provided from supporting elements during the engineering planning and installation phases of new or reconfigured computer facilities.
- c. Ensure that contractual documents for those contracts involving the use of computer facilities to process national defense information include appropriate TEMPEST provisions. CMC (CSBT) will provide advice and assistance, as requested, in formulating contractual TEMPEST provisions.
- d. Before any system processing classified information can be accredited, a TCR is required (see exception in para 8.3.c) to be submitted to NISE EAST in accordance with OPNAVINST C5510.93. This represents only one step of the accreditation process. Once the TCR is received by NISE EAST, a determination will be made, based upon the information provided, to identify the system/equipment as either an acceptable risk or to schedule an Instrumented TEMPEST Survey (ITS).
- e. DAA's should not accredit systems designed or acquired to process classified information unless a TCR (see exception in para 8.3.c) has been submitted.

8.5. TEMPEST CONTROLS There are basically four methods recommended for controlling compromising emanations:

- a. To provide the equipment with a physical control zone (PCZ) of sufficient spherical diameter to preclude successful hostile intercept action.

b. To implement minimum essential countermeasures to contain compromising signals within the accepted PCZ.

c. To design or modify the equipment to limit the strength of compromising signal to acceptable limits within the available PCZ.

d. To purchase products from the Preferred Products List (PPL) contained in the NSA Information Systems Security Products and Services Catalogue. The catalogue is updated quarterly to announce new products as well as removing any product containing confirmed deficiencies.

(1) To decide which of the foregoing is necessary, the equipment must be tested. If the equipment has not been previously tested, it may be tested by having an onsite survey conducted by NISE EAST technicians.

(2) A PCZ does not automatically require a fenced, guarded area or closed-circuit surveillance system. Only under the most unusual circumstances will that action be necessary purely for TEMPEST security.

(3) Any computer equipment may cause TEMPEST emanations. The type of equipment which may be expected to produce the worst radiation includes input/output devices in which the circuits creating or transferring data operate at high voltage or current levels. Video Display Terminal devices of the type requiring reiterative refreshing of the viewing screen and associated buffers may require a very large control zone if installed in an open environment and not modified to restrict radiated or conducted signals.

8.6. FILTERED POWER Computer equipment which does not meet TEMPEST requirements may require filtered power. The decision to provide filtered power normally will be based on the location and configuration of the primary source; the degree of control exercised over the primary power sources; the power lines/cables to the computer equipment; and other equipment/facilities supported from the same primary power source.

8.7. TEMPEST COUNTERMEASURES The TEMPEST countermeasures required for your facility can be determined by using NISE EAST TEMPEST Alternatives Determination

Procedures available from Navy Electronic System Security Engineering Center (NESSEC) Code 04. It is emphasized here that the need for a Preferred Products List (PPL) item or a shielded enclosure must be coordinated with and or approved by NESSEC Code 04, prior to implementation.

a. If your facility is already in operation no changes to implement TEMPEST countermeasures should be made until your TCR has been evaluated. A copy of any countermeasures determination data should be attached to your TCR submittal. If you are planning a new facility, NESSEC should be contacted for support in determining your TEMPEST countermeasure requirements.

8.8. PROTECTED DISTRIBUTION SYSTEM (PDS) An additional area of concern - one which receives very little attention - is the requirement that any distributed system must use an approved PDS for its interconnecting wirelines (in accordance with OPNAVINST C5510.93), if they will extend beyond the boundary of the controlled space within which the processing equipments are located. In all cases, the PDS must be technically reviewed by NESSEC Code 04 and approved by appropriate authority as stated in OPNAVINST C5510.93.

Chapter Table of Contents

Chapter 9

CLASSIFIED PROCESSING

Paragraph Page

Section 1. <u>INFORMATION</u>	9.1. 9-3
Background	9.1.1. 9-3
Section 2. <u>APPLICABLE TERMS</u>	9.2. 9-3
Section 3. <u>TEMPEST COUNTERMEASURE REVIEW</u> <u>(TCR) REQUIREMENT</u>	9.3. 9-4
TCR Submittal	9.3.1. 9-5
TCR Format	9.3.2. 9-5
Exceptions To National Policy	9.3.3. 9-5
Sensitive Compartmented Information (SCI)	9.3.4. 9-5
Section 4. <u>SYSTEM ACCREDITATION/LABELS</u>	9.4. 9-6
Accreditation Review	9.4.1. 9-6
Accreditation Labels	9.4.2. 9-6

Section 5. <u>CLASSIFIED MEDIA MARKING</u>	9.5. 9-6
Floppy Diskettes	9.5.1. 9-6
Other Magnetic Media	9.5.2. 9-6
Accountability	9.5.3. 9-6
Hardcopy Reports	9.5.4. 9-7
Printer Ribbons	9.5.5. 9-7

(This page intentionally left blank)

Chapter 9

CLASSIFIED PROCESSING

9.1. INFORMATION This chapter establishes security procedures for Mini and Microcomputer systems (except where main-frames are denoted) used to process classified information.

9.1.1. Background As a result of the ever increasing use of Mini and Microcomputers in the Marine Corps, it has become necessary to provide definitive security procedures to ensure all classified information processed in these computers is adequately protected. Security and administrative procedures in this chapter are based upon National Defense and Department of the Navy standards and requirements in the following directives; NACSIM 5100A, NACSEM 5100, OPNAVINST C5510.93, and MCO P5510.14.

9.2. APPLICABLE TERMS Managers and personnel responsible for classified processing should become familiar with the terminology contained below:

a. Classified Information Processing System (CLIPS) Any equipment, device or system which is electrically powered and processes, converts, reproduces, or otherwise manipulates any form of classified information. The following types of equipment are typical: electrical or electronic typewriters; reproduction copiers; word processors; composing and editing equipment; video displays; micro, mini, and main-frame computers; telecommunications equipment and systems including the teletype, facsimile, and cryptographic equipment; and all interfaces, power sources, and interconnecting paths which are part of the system or equipment.

b. Controlled Space (CS) The three-dimensional space surrounding equipment that process classified information within which unauthorized personnel are denied unrestricted access or are escorted by authorized personnel or are under continual surveillance. The spaces should be controlled at levels equivalent to the data processed/stored within the spaces. Thus a facility can have Confidential, Secret, Top Secret or Compartmented controlled spaces. If a Top Secret or Compartmented controlled space is bordered by a Secret controlled space, the Secret controlled space is usually adequate protection for compromising emanations, even if the compromising emanations would reveal Top Secret or Compartmented information. The primary condition under which this does not hold is if the compromising emanations could be read unintentionally due to both the nature of the compromising emanations and the equipment or operating procedures in use in the secret controlled space. For shore fixed-plants, mobile and transportable CLIPS, Department of the Navy (DON) controlled spaces are defined as areas under the positive control of a command or activity. Positive control requires that all personnel not cleared to the

level of the data processed within the space are under continual escort by cleared personnel or under continual surveillance such that any covert or overt attempt to exploit an emanating signal would be immediately detected. Multiple controlled spaces may be treated as a single controlled space as long as there are no uncontrolled areas within the overall boundaries of the contiguous space.

c. TEMPEST-Accredited CLIPS A CLIPS which is designed for TEMPEST and meets a stringent set of laboratory TEMPEST standards based on qualification testing and can be installed in almost any environment without presenting a TEMPEST problem. The manufacturer guarantees to support the TEMPEST posture of these devices. All computers and supporting peripheral equipment listed in the Preferred Products List (PPL) fall into this category although all equipment in this category may not be listed in the PPL for reasons given in that publication. The PPL is a subset of the NSA prepared "Information Systems Security Products and Services Catalogue" available through subscription from the Government Printing Office (GPO).

d. TEMPEST-Approved CLIPS A CLIPS which is not designed for TEMPEST (sometimes marketed as "designed to meet NACSIM 5100A") but meets a selected set of minimum TEMPEST requirements based on statistical evaluation of field or laboratory testing and can be installed in certain general environments without presenting a TEMPEST problem. The manufacturer will not necessarily maintain the TEMPEST posture of these devices. These devices are not authorized for Marine Corps processing.

e. TEMPEST-Certified CLIPS A CLIPS which has been evaluated in a specific location and which does not cause a TEMPEST problem. The CLIPS may or may not meet any specific TEMPEST standards. It may have extremely strong compromising emanations, but may be certified due to a large controlled space. These devices are not recommended.

f. Security Modes A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS. Appendix F addresses the security modes of operation minimum requirements and how they relate to the Trusted Systems Criteria, DOD Standard 5200.28-STD.

9.3. TEMPEST COUNTERMEASURE REVIEW (TCR) REQUIREMENT Prior to use in processing classified information or as soon as possible after the start of classified processing, all commands will submit a TCR (See Chapter 8, paragraph 8.3.c, for exceptions) for all main-frame, mini and microcomputer systems. In assessing the TCR, NISE EAST will designate the system as

an acceptable risk or, to ensure the system is TEMPEST certified, assign an

Instrumented TEMPEST Survey (ITS). If NISE EAST determines that upon completion of the TCR that an ITS is required, then NISE EAST will assign a priority for conducting that survey. NISE EAST will respond by message or letter to all units submitting TCRS with the assigned survey priority (if required) and the security classification processing level authorized for each system. When the processing level of a system changes, a new TCR must be submitted.

9.3.1. TCR Submittal All commands are directed to submit a TCR in accordance with OPNAVNOTE C5510ser 09N/4C535007 dated 14 Apr 94 until OPNAVINST C5510.93E has been updated. A TCR must be submitted prior to processing classified information to:

Naval Command Control and Ocean Surveillance Center
ISE East Detachment Washington, Code NE42
3801 Nebraska Ave NW
Washington, DC 20393-5454

9.3.2. TCR Format The format for submitting a TCR for all computer systems is contained in OPNAVNOTE C5510ser 09N/4C535007 dated 14 Apr 94.

9.3.3. Exceptions to the National Policy Exceptions to the National Policy on Compromising Emanations are required as set forth in Section II of enclosure (4) of OPNAVINST C5510.93. Request for exceptions will be submitted by message within 30 days of the ITS. This message must be classified SECRET. Forward request to NISE EAST via CMC (Code CSBT) with a copy to CO, NAVELEXSECCEN, and any other appropriate command.

9.3.4. Sensitive Compartmented Information (SCI) Systems used for processing Sensitive Compartmented Information (SCI) must first have a Technical Surveillance Countermeasures (TSCM) inspection prior to placement in the SCI Facility (SCIF). Request for TSCM inspections should be submitted through the Special Security Office (SSO) to the nearest Counter Intelligence Team (CIT). Additionally, TCR's for systems processing SCI will be forwarded to NISE EAST with a info copy to NAVELEXSECCEN and CMC (code CSB). NISE EAST may authorize processing of information up to Top Secret. An authorization from NISE EAST will be forwarded with a copy of the TCR to CNO (OP-OO9P) for accreditation of the computer system to process SCI in the SCIF.

9.4. SYSTEM ACCREDITATION/LABELS System accreditation will not become effective until a formal, dated, Statement of Accreditation has been issued by the DAA as a result of a system accreditation review.

9.4.1. Accreditation Review The statement of system accreditation will include the specified level of sensitivity or classification for which the accreditation is based, a statement by the DAA as to the acceptability of identified risks (where applicable), and any exceptional circumstances incumbent to system accreditation. This brief statement should be adequate for purposes of subsequent system accreditation reviews and re-accreditation (every three years). Chapter 2 defines the approval authority depending on the sensitivity level of the data processing on the system.

9.4.2. 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, or have received the DAA's interim authority to process classified information (to include a formal TCR), 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 or interim authority to operate. System accreditation labels are available through normal Marine Corps supply channels. Stock numbers for ordering accreditation labels are contained in Appendix C.

9.5. CLASSIFIED MEDIA MARKING All removable or transportable magnetic media on which classified information is stored must be color coded or marked with a label (sticker) indicating the classification and special access category of the recorded information. In those instances where it is not practical to label the media itself, the container in which it is stored must be labeled.

9.5.1. Floppy Diskettes All floppy diskettes used for Classified processing will be color coded (according to the color scheme in Appendix C) to the highest classification of the information on them. Classified color coded diskettes with labeling information already embossed can be ordered through normal Marine Corps supply channels and are listed in Appendix C.

9.5.2. Other Magnetic Media All other types of removable magnetic media (such as removable hard disks or cassette tapes) will be labeled with a color coded label (sticker) as identified and listed in Appendix C. Color coded labels and the Data Descriptor label are available through normal Marine Corps supply channels. Stock numbers for ordering the labels are contained in Appendix C.

9.5.3. Accountability All magnetic media which contain classified data will be accounted for by the highest classification of data that they have ever contained in accordance with OPNAVINST 5510.1 (non-SCI), DoD C-5105.21-M-1 (SCI), and local procedures. Media will be declassified or destroyed in accordance with CSC-STD-005-85 DoD Magnetic Remanence Security Guideline." Classified information handling procedures are contained in Appendix C.

9.5.4. Hardcopy Reports Hardcopy reports or printouts from a line printer, terminal, plotter, or other computer-based system will be marked as follows:

a. Reports prepared during classified processing will be marked at the top and bottom of each page with the appropriate classification or the word "UNCLASSIFIED."

b. Page numbering and binding of classified reports are to be used when possible. Forewords, prefaces, or special instructions may be bound as a computer report, but will be in a separately numbered section or distinguished by Roman numeral page numbers to avoid renumbering of machine numbered pages.

c. Computer output microfilm/microfiche will be machine marked the same as described for hard copy reports.

d. All classified monitors (CRT displays) will have the appropriate security classification markings displayed at the top of the screen. Hard copy reports generated from such a device will be marked as cited above.

9.5.5. Printer Ribbons Due to the large variety of ribbons and printers in use, it is difficult to state with certainty that any and all classified information has been totally obscured from a given ribbon without a detailed examination of that ribbon.

a. Printer ribbons should be controlled at the highest level of information ever printed by that ribbon until that ribbon is destroyed.

b. The same ribbon should be retained in the printer for unclassified and classified information consistent with the levels of physical security enforced for the work area.

c. Laser technology printers used for both unclassified and classified printing can be sanitized by simply printing three blank pages after the last classified page has printed. However, laser printer parts, (i.e., cartridges, drums, and belts, etc.), regardless of classified or unclassified processing, must be disposed of IAW classified destruction procedures. This will ensure that any residue left from previous classified printing will not be compromised.

Chapter Table of Contents

Chapter 10

TECHNICAL VULNERABILITY REPORTING

Paragraph Page

Section 1. <u>INFORMATION</u>	10.1. 10-3
Section 2. <u>BACKGROUND</u>	10.2. 10-3
Section 3. <u>APPLICABILITY AND SCOPE</u>	10.3. 10-3
Section 4. <u>REPORTING PROCEDURES</u>	10.4. 10-3
Report Format	10.4.1. 10-3
Report Validation	10.4.2. 10-4
Report Submission	10.4.3. 10-4
Section 5. <u>NISAC REPORTS/BULLETINS</u>	10.5. 10-4
Section 6. <u>PRODUCT EVALUATION</u>	10.6. 10-4

(This page intentionally left blank)

Chapter 10

TECHNICAL VULNERABILITY REPORTING

10.1. INFORMATION DoD Instruction 5215.2 established the Computer Security Technical Vulnerability Reporting Program (CSTVRP) under the direction of the National Security Agency (NSA), National Computer Security Center (NCSC), as a means for reporting all demonstrable and repeatable technical vulnerabilities of computer systems. CSTVRP provides for collection, consolidation, analysis, reporting, or notification of generic technical vulnerabilities and dissemination of corrective measures.

10.2. BACKGROUND A technical vulnerability is a hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation either externally or internally, resulting in risk of compromise of information, alteration, destruction of information, or denial of service. Technical vulnerability information, if made available to unauthorized persons, may allow a computer system to be exploited.

10.3. APPLICABILITY AND SCOPE The DoD program is focused on technical vulnerabilities in commercially available hardware, firmware and software products acquired by the Marine Corps and those altered commercial products supporting standard military applications. This also includes technical vulnerabilities in products on the National Computer Security Center (NCSC) Evaluated Products List (EPL), which have been certified and given a trusted system rating. Embedded computer systems, research prototypes and reproduction commercial products are excluded from the program.

10.4. REPORTING PROCEDURES Technical vulnerabilities shall be reported to CMC (Code CSBT) by message or letter and must be classified at the highest classification level of information accessible by the vulnerability, but at least For Official Use only. Since unauthorized access to technical vulnerability information can lead to exploitation of a Marine Corps computer system, release of this information must be based on a validated security clearance and need-to-know. Technical vulnerability information must not be released to foreign nationals.

10.4.1. Report Format Reports of technical vulnerabilities should be in sufficient detail so the vulnerability can be demonstrated and repeated. Appendix H contains the format and the categories of information for reporting a technical vulnerability. Compliance with the DoD program does not preclude the responsibility to take any necessary and prudent action to reduce any risk presented by the vulnerability.

10.4.2. Report Validation All vulnerability reports received by CMC (Code CSBT) will be forwarded to CDA, Quantico to be screened for technical validity and determine the extent of risk presented by the technical vulnerability to other Marine Corps sites.

10.4.3. Report Submission Within four weeks of receipt of a valid vulnerability, CMC (Code CSBT) will submit the original report to the NCSC with a summary of the reported vulnerability and any analysis of the risk involved. This report will be entered into the NCSC data base and forwarded to the NCSC for analysis and resolution. If the product is on the EPL, NCSC will evaluate the risk and make a specific determination as to whether or not to retain, reduce, or rescind the product from its current trusted system rating. If a product rating is changed, appropriate warnings will be submitted to the DoD focal points (CMC contact is Code CSB) for dissemination.

10.5. NCSC REPORTS/BULLETINS NCSC will report their findings on the technical vulnerability being analyzed to NCSC for reporting back to the originator. A technical vulnerability report with findings and recommended solutions will be submitted by the NCSC to CMC (Code CSBT). CMC will then contact the Marine Corps organization submitting the report with guidance to resolve the vulnerability. Technical vulnerabilities affecting more than the Marine Corps will be disseminated in a classified bulletin by the NCSC to the appropriate DoD component focal points.

10.6. PRODUCT EVALUATION When a technical vulnerability in a reported product has been confirmed, NCSC may request that the responsible vendor correct the identified vulnerability. Any technical vulnerability found in products appearing on the EPL will be immediately referred by NCSC to the responsible vendor for correction. NCSC may provide vendors the technical details of reported vulnerabilities to make corrections, but shall not include information about the specific site(s) concerned, methods of discovery, or other information which could lead to increased site vulnerability. In all cases, NCSC will publish a classified bulletin announcing any technical vulnerability in a product. In this regard, NCSC will also announce via a bulletin when the vendor has corrected the vulnerability with its product and when the product will be recertified by the NCSC.

Chapter Table of Contents

Chapter 11

NETWORK SECURITY

Paragraph Page

Section 1. <u>INFORMATION</u>	11.1. 11-3
Section 2. <u>DATA NETWORKS</u>	11.2. 11-3
Section 3. <u>MINIMUM REQUIREMENTS</u>	11.3. 11-3
Interservice And Interagency Networks	11.3.1. 11-3
Section 4. <u>NETWORK ACCESS</u>	11.4. 11-3
Terminal And System Security	11.4.1. 11-3
Access Attempts	11.4.2. 11-4
Call Back Systems	11.4.3. 11-4
Audit Trails	11.4.4. 11-4
Automatic Termination	11.4.5. 11-4
Section 5. <u>NETWORK PROTECTION</u>	11.5. 11-4
Section 6. <u>DIAL-UP ACCESS</u>	11.6. 11-4

Dial-Up Access To MCDN	11.6.1. 11-4
Asynchronous Dial-Up (Class C2 or Above)	11.6.2. 11-6
Asynchronous Dial-Up (Non-Class C2)	11.6.3. 11-6
Establishing Asynchronous Dial-Up Communications	11.6.4. 11-6
Use of Non-Standard Dial-Up Products	11.6.5. 11-6

(This page intentionally left blank)

Chapter 11

NETWORK SECURITY

11.1. INFORMATION This chapter defines additional security measures when systems link with other systems or terminals access systems through a telecommunications network.

11.2. DATA NETWORKS Any interconnection of computers and terminals via communications lines is considered a data network for security purposes. Sensitive, classified, proprietary, critical, or privileged information on networks may be vulnerable to disclosure through taps, manipulation of network interfaces or components, and emanations. Unauthorized access to a system through a network may also result in compromise or modification of information. Security concerns for Local and Wide Area Networks are addressed in IRM-5239-04.

11.3. MINIMUM REQUIREMENTS The mechanisms and procedures to protect information and processes must at least complement and should enhance the security provided in the networked terminals and systems.

a. The DAA for networks that pass sensitive information shall designate a Network Security Officer (NSO). Each network shall be accredited by the DAA to operate at the maximum specified level of sensitivity.

b. Each NSO must maintain a record of authorized users of a network and their network privileges. The record may be automated or manual.

c. Each NSO must limit knowledge of access codes, telephone numbers, passwords, etc., to those with a need to know.

d. A risk assessment is mandatory for the network. The assessment must include each component of the network. This assessment becomes part of the accreditation documentation that is required by the DAA to determine if the network is worthy of accreditation.

11.3.1. Interservice And Interagency Networks Organizations that depend on interservice or interagency networks should develop a Memorandum of Agreement (MOA) for each AIS networked with another service or agency system and forward it to each command, service or agency DAA for review and mutual acceptance.

11.4. NETWORK ACCESS

11.4.1. Terminal And System Security Limit access to networked terminals and systems commensurate with the highest sensitivity and criticality of the data processed. It is especially critical to protect the access mechanisms used by the terminals and systems.

11.4.2. Access Attempts Limit the number of unsuccessful attempts to access a network or networked system and lock out further attempts. Allow three attempts for networks processing unclassified information, two for classified. At a minimum, lock out the user-ID; and if possible, lock out the terminal. When a lock out occurs, notify the NSO or system operator. Only the NSO, CSSO, computer security staff or TASO administrator can authorize access reinstatement. Enforce these restrictions at each point in the network where access controls are applied (i.e., gateways, hosts).

11.4.3. Call Back Systems Call back systems provide marginal access protection. Do not use telephones with call forwarding capability in call back systems.

11.4.4. Audit Trails Maintain audit trails on all security related activities. Audit trails may be automated or manual and should be reviewed periodically for security violations. At a minimum, an audit trail must include login procedures, auditing of security-relevant events, and resource isolation that allows a computer system to be identified to a network.

11.4.5. Automatic Termination Networks and systems must automatically terminate sessions after periods of inactivity. The length of time will depend on the sensitivity of the information processed by the host system. When the network initiated the disconnect, the host must be able to detect the event and automatically log-out the user to prevent unauthorized access through the session.

11.5. NETWORK PROTECTION Information, including users IDs and passwords transmitted on a network is vulnerable to unauthorized disclosure. Mechanisms to prevent compromise of

classified and sensitive unclassified information are mandatory. Protection levels and associated requirements for data and devices are described in Appendices E, F, and G. Detailed guidance for required protection (minimum level is Class C2 for sensitive unclassified systems) to operate trusted systems/networks is contained in DoD Standards 5200.28-STD "DoD Trusted Computer System Evaluation Criteria", and NCSC-TG-005 "Trusted Network Interpretation." Refer to Appendix C for ordering these DoD documents.

11.6. DIAL-UP ACCESS All Dial-up circuits to Marine Corps systems will be secured according to the requirements specified below.

11.6.1. Dial-Up Access To MCDN Dial-up circuits used to gain access to applications which run on MCDN hosts will be supported in the following manner:

a. All Dial-up communications will be controlled through:

- ACF/VTAM using IBM's Synchronous Data Link Control (SDLC) protocol or,
- authorized asynchronous methods described in paragraph 11.6.4. or,
- approved alternatives as stated in paragraph 11.6.5.

b. All dial-up access into MCDN must be approved by MCCDC (Code AS) prior to implementation.

c. Network Software Associates, Inc.'s Adaptasynch has been evaluated by the Marine Corps Central Design Activity (CDA) Quantico and has been determined to provide the necessary security requirements for entry into MCDN for asynchronous terminals.

d. Dial-up access using the SDLC protocol or Adaptasynch will adhere to the following:

(1) All dial-up resources will be named using MCDN naming standards as specified in IRM-5234-07, DATA CENTER IDENTIFICATION STANDARDS. That is, dial-up terminal resource ID's will have a "D" in their third position (e.g., GGD74A00).

(2) All dial-up resources will be defined as TERMINALS and controlled by CA-Top Secret (CA-TSS). Ownership of these resources (i.e. TERMINALS) will be assigned to the CSSO of the local MCDN host computer.

(3) All non-LAN dial-up access will be accomplished by dialing into a port on a front end processor (FEP) at a MCDN node (i.e., physical unit type 4). VTAM is the authentication system used for SDLC dial-up and Adaptasynch is used for asynchronous dial-up.

e. All dial-up access from remote sites using asynchronous communications to the MCDN via a Local Area Network (LAN) will adhere to the following:

(1) LANs and microcomputers which have connections into MCDN may be configured to allow dial-up access into MCDN via the connection using the asynchronous protocol Banyan Vines "PC Dial-In" or an approved alternative; (Paragraphs 11.6.4. and 11.6.5. apply).

(2) MCDN nodes are responsible for ensuring compliance with this provision prior to providing a connection to MCDN. The node will review the LAN's and microcomputer's configuration for compliance. Nodes will periodically audit LANs and microcomputers connected to their MCDN node in support of the site accreditation process.

f. Minicomputers, word processors and office automation equipment, excluding LAN servers, configured to emulate IBM 3270 control units (i.e., physical unit types 1 & 2) will not be configured to allow dial-up access into MCDN through their ports. MCDN nodes are responsible for ensuring compliance with this provision through regular audits and inspections of their subnetworks. These audits and inspections will be included in the site accreditation process required by MCO P5510.14.

g. AIS applications designed to run on MCDN hosts will be designed so that they use standard, formatted IBM 3270 screens. Unformatted screens will not be used.

11.6.2. Asynchronous Dial-Up (Class C2 or Above) Asynchronous Dial-up circuits that allow access to other computer-based systems (e.g., microcomputers, maintenance ports on

communication processors and mainframes, local area networks, etc.), which have been certified to meet Class C2 or above criteria as specified in DoD 5200.28-STD, require no additional security provided the Class C2 features and functions have been fully and effectively implemented.

11.6.3. Asynchronous Dial-Up (Non-Class C2) Asynchronous dial-up circuits that allow access to other computer-based systems which have not been certified to meet the Class C2 or above criteria in DoD 5200.28-STD or where the Class C2 features and functions have not been implemented, will be secured in one of the following ways:

a. Dial-up communication ports will be protected using an authentication or encryption device which requires unique identification and accountability of authorized dial-up users.

b. If no authentication or encryption device is used, communication ports will be disconnected from the circuit when not in use in a manner which prevents unmonitored dial-up access. Auto-answer modems will not be used unless the circuit is physically disconnected from the modem when a session is not active.

11.6.4. Establishing Asynchronous Dial-Up Communications

a. The only approved Marine Corps method of establishing asynchronous dial-up communications to a LAN or to MCDN through a LAN is the Banyan Vines "PC Dial-In" option.

b. The minimum password length for a Banyan Vines account is seven characters and must be changed at least every 30 days. This restriction should be established at the group security level.

c. Users requiring dial-up access must be explicitly granted permission for such access.

d. No automatic logon and password entry procedures are authorized.

11.6.5. Use of Non-Standard Dial-up Products Marine Corps organizations desiring to procure products for asynchronous communications other than the Banyan Vines "PC Dial-In" option or Network Software Associates' Adaptasynch, must provide justification to MCCDC (Code AS) for

approval prior to implementation. The alternative product justification should clearly state the functionality that is not provided by the "PC Dial-In" option of Adaptsynch that necessitates the request and should describe the product and its security features.

(This page left intentionally blank)

Appendix A

GLOSSARY OF ACRONYMS AND TERMS

PART I: ACRONYMS

ADP Automated Data Processing

AIS Automated Information System

COMPUSEC Computer Security

COMSEC Communications Security

CPU Central Processing Unit

CSSO Computer Systems Security Officer

CSTVRP Computer Security Technical Vulnerability Reporting Program

DAA Designated Approving Authority

DES Data Encryption Standard

DIAM Defense Intelligence Agency Manual

DoD Department of Defense

EPL Evaluated Products List

FWA Fraud, Waste and Abuse

GENSER General Services

GPO Government Printing Office

GSA General Services Administration

ITS Instrumented TEMPEST Survey

ITT Instrumented TEMPEST Test

LAN Local Area Network

LCM Life-Cycle Management

NAC National Agency Check

NACSI National COMSEC Instruction

NACSIM National COMSEC Information Memorandum

NCSC National Computer Security Center

NSA National Security Agency

NSO Network Security Officer

NTISSC National Telecommunication and Information System Security Committee

OPSEC Operations Security

PDS Protected Distribution System

PL Public Law

PPL Preferred Products List

SAISS Subcommittee on AIS Systems Security of NTISSC

SCI Sensitive Compartmented Information

SDLC Synchronous Data Link Control

SIOP-ESI Single Integrated Operational Plan-Extremely Sensitive Information

ST&E Security Test and Evaluation

STS Subcommittee on Telecommunications Security of NTISSC

TASO Terminal Area Security Officer

TCB Trusted Computer Base

TCSEC DoD Trusted Computer System Evaluation Criteria

TEMPEST Compromising Emanations

USER-ID User Identification

PART II: TERMS

ACCESS - A user's ability to communicate with (input to or receive output from) a system or to have entry to a specified area.

ACCESS CONTROL - The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

ACCESS CONTROL MECHANISM - Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

ACCOUNTABILITY - The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

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.

ACCREDITATION AUTHORITY - Synonymous with Designated Approving Authority.

ADD-ON SECURITY - The retrofitting of protection mechanisms, implemented by hardware and software.

AUTHENTICATE - To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

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.

AVAILABILITY OF DATA - The state when data are in place needed by the user, at the time the user needs them, and in the form needed by the user.

BLACK - Refers to unclassified information or equipment and wire lines that handle encrypted classified information.

CALL BACK - A procedure for identifying a remote device. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote device to reestablish the connection. Synonymous with dial-back.

CATEGORY - A restrictive label that has been applied to classified or unclassified data as a means of increasing the protection of the data and further restricting access to the data.

CERTIFICATION - The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

COMMUNICATIONS SECURITY (COMSEC) - Measures taken to deny unauthorized persons

information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material and information.

COMPARTMENT - A class of information that has need-to-know access controls beyond those normally provided for access to Confidential, Secret or Top Secret information.

COMPUTER - A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices.

CONFIDENTIALITY - The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

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 facilitate the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan.

CONTROL ZONE - The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude an unauthorized entry or compromise.

COUNTERMEASURE - Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.

DATA AGGREGATION - The result of assembling or combining distinct units of data when handling sensitive information. Aggregation of data at one sensitivity level may result in the total data being designated a higher sensitivity level.

DATA ENCRYPTION STANDARD (DES) - A cryptographic algorithm for the protection of unclassified data, published in U.S. Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and

government use.

DEGAUSSER - An electrical device that can generate a magnetic field for the purpose of degaussing magnetic storage media.

DEGAUSSER PRODUCTS LIST (DPL) - A list of commercially produced degaussers that meet National Security Agency specifications. This list is included in the NSA Information Systems Security Products and Services Catalogue, and is available through the U.S. Government Printing Office.

DENIAL OF SERVICE - Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

DESIGNATED APPROVING AUTHORITY (DAA) - The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

DISCRETIONARY ACCESS CONTROL - A means of restricting access to information based on the identity and need-to-know of the user, process and/or groups to which they belong.

DOD TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC) - A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store classified or Sensitive Unclassified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as "The Criteria" or "The Orange Book."

EMISSION SECURITY - The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems.

EVALUATED PRODUCTS LIST (EPL) - A list of equipments, hardware, software, and/or firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DOD TCSEC by the NCSC. The EPL is included in the NSA Information Systems Security Products and Services Catalog, which is available through the U.S. Government Printing Office.

FORMAL ACCESS APPROVAL - Documented approval by a data owner to allow access to a particular category of information.

INTERNAL SECURITY CONTROLS - Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices).

LEAST PRIVILEGE - The principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from error or unauthorized use.

LOGIC BOMB - A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized.

MAGNETIC REMANENCE - A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.

MALICIOUS LOGIC - Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e.g., a Trojan horse.

MANDATORY ACCESS CONTROL - The result of a system that preserves the sensitivity labels of major data structures in the system and uses them to enforce mandatory access controls.

NATIONAL COMPUTER SECURITY CENTER (NCSC) - Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the U.S. Government.

OBJECT REUSE - The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media.

OPERATIONS SECURITY (OPSEC) - An analytical process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

ORANGE BOOK - Alternate name for DoD Trusted Computer System Evaluation Criteria.

PERSONNEL SECURITY - The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.

PHYSICAL SECURITY - The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

PREFERRED PRODUCTS LIST (PPL) - A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by the NSA. This list is included in the NSA Information Systems and Services Catalogue, and available through the GPO.

PROCEDURAL SECURITY - The management constraints and supplemental controls established to provide an acceptable level of protection for data.

PUBLIC DOMAIN - Software that is not proprietary or copyrighted.

PUBLIC LAW 100-235 - Also known as the Computer Security Act of 1987, this law creates a means for establishing minimum acceptable security practices for improving the security and privacy of Sensitive Unclassified information in federal computer systems. The law also requires establishment of security plans by all operators of federal computer systems that contain Sensitive Unclassified information.

RED - Refers to equipment and wire lines handling nonencrypted, classified information.

RESIDUAL RISK - The portion of risk that remains after security measures have been applied.

RISK ASSESSMENT - The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk assessment is a part of risk management.

SECURITY EVALUATION - An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information.

SECURITY FLAW - An error of commission or omission in a system that may allow protection mechanisms to be bypassed.

SECURITY POLICY - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

SECURITY REQUIREMENTS - The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

SECURITY SAFEGUARDS - The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include; hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

SECURITY TEST AND EVALUATION (ST&E) - The process to determine that the system administrative, technical, and physical security measures are adequate; to document and report test findings to appropriate authorities; and to make recommendations based on test results.

SENSITIVE UNCLASSIFIED INFORMATION - Any unclassified information, the loss, misuse, modification of, or unauthorized access to, could adversely affect the national interest or the conduct of U.S. programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code (The Privacy Act).

SOFTWARE SECURITY - General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system.

SYSTEM INTEGRITY - The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

TECHNICAL VULNERABILITY - A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

TRAP DOOR - A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented in some innocent-appearing manner; e.g., a special "random" key sequence at a keyboard. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with back door.

TROJAN HORSE - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

TRUSTED COMPUTER SYSTEM - A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of classified or Sensitive Unclassified information.

TRUSTED COMPUTING BASE (TCB) - The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system.

TRUSTED SOFTWARE - The software portion of the TCB.

USER ID - A unique symbol or character string that is used by a system to identify a specific authorized user.

VIRUS - A computer program with the ability to replicate itself usually by attaching itself to other programs to the detriment of security and integrity. May or may not be introduced through a Trojan Horse.

Appendix B

REFERENCES

1. OMB Circular A-130, Management of Federal Information Resources.
2. Public Law 102-561, Copyright Infringement of 1992
3. Public Law 100-235, Computer Security Act of 1987.
4. Public Law 99-474, Computer Fraud and Abuse Act of 1986.
5. Public Law 97-255, Federal Manager's Financial Integrity Act of 1982.
6. Public Law 93-579, The Privacy Act of 1974.
7. DOD Directive 5200.28, Security Requirements for AIS's.
8. DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (Orange Book).
9. DOD Directive 5215.1, Computer Security Evaluation Center.
10. DOD Directive 5215.2, Computer Security Technical Vulnerability Reporting Program.
11. CSC-STD-005-85, Magnetic Remanence Security Guideline.
12. NCSC-TG-005, Trusted Network Interpretation.

13. SECNAVINST 5239.2, Department of the Navy AIS Security Program.

14. SECNAVINST 5370.2, Standards of Conduct and Government Ethics.

15. OPNAVINST 5239.1A, Department of the Navy ADP Security Program.

16. OPNAVINST 5510.1, Department of the Navy Information and Personnel Security Program Regulation.

17. OPNAVINST C5510.93, Navy Implementation of the National Policy on Compromising Emanations (U).

18. OPNAVINST 5530.14, DON Physical Security and Loss Prevention.

19. MCO P5510.14, Marine Corps ADP Security Manual.

20. MCO P5231.1, Life Cycle Management for AIS Projects.

Appendix C

CLASSIFIED MEDIA AND EXTERNAL LABELS

INTRODUCTION. This appendix is provided as a quick reference look-up for detailed information that is required in support of classified and sensitive processing procedures. It also includes guidance for ordering color coded diskettes, magnetic media labels, accreditation labels and DOD sponsored NSA/NCSC published guides.

1. CONTROL AND ACCOUNTABILITY MEASURES. Responsible organizations should implement security controls in accordance with OPNAVINST 5510.1 for classified ADP media to include, but not limited to, the following:

a. Maintenance of an ADP media log to provide a complete inventory of classified media and files to include classification, media catalog number or file name, owner date created, date declassified or destroyed.

b. Mark externally all media with highest classification thereon.

c. Mark internally all files with classification authority, date created, owner and classification.

d. Store all classified media in GSA approved security containers when not in use.

e. Systems with internal hard disk or other internal mass storage media should be stored in a manner which provides the appropriate level of security for data resident in internal memory.

f. Computer monitors should be inspected for burn-in. Consider usage of screen blanking software.

g. When disposing of or declassifying media, ensure that special procedures as they relate to the specific media involved are followed, i.e., degaussing magnetic media, overwriting mass storage media, burning or shredding of floppy disks, replacement and destruction of monitors with

classified information burned into the screen.

h. Establish provisions for emergency destruction of ADP media or resident data.

2. PHYSICAL AND PERSONNEL MEASURES. Specific security measures should be implemented to prevent or minimize the effects of any natural, accidental or malicious event on computer systems.

These measures include but should not be limited to the following:

a. Limiting users to those with proper clearance and need to perform work on the system.

b. Identifying authorized users by placing an updated authorized users list in an easily observed location.

c. Screening individuals for disciplinary or behavioral problems prior to use.

d. Revoking authorizations of personnel who have become disciplinary or behavioral problems, and denying access of these personnel to rooms or compartments containing computers used for classified processing.

e. Ensuring personnel performing maintenance are authorized to perform the level of maintenance required. In those cases when equipment must be removed from a secure location to perform maintenance, equipment must be fully declassified prior to its move. Ensure personnel entering secure compartments to perform maintenance have an appropriate security clearance.

f. Maintaining an accurate and up-to-date inventory of all hardware and software by serial number and location.

3. SYSTEM SECURITY MEASURES. The following guidance is provided for system security:

a. Systems will be operated in "Systems High Mode". That means when the system is processing classified information, only those individuals possessing the requisite clearance for the highest classification of data in the system (or any media accessible through the system), and possessing the need-to-know for any of the information accessible through the system, will be allowed access.

b. Systems must be afforded that level of protection required by the highest classification of data processed by the system.

c. Each component of the system will be powered on and off at least three times before processing a different level of classification, such as changing from system high of Secret to system high of Confidential.

d. Systems containing integral hard disks should not be used to process classified information. However, if no alternative exists, the system must be protected and physically secured at all times at the level afforded the highest classification of data ever processed on the system (See paragraph 4 below for procedures). These systems will be declassified or downgraded and will be handled in accordance with CSC-STD-005-85, DOD Magnetic Remanence Guideline.

e. Privately owned systems are not authorized to process classified information. Additionally, privately owned software or public domain software from non-government sources is not authorized to process classified information. This security measure is intended to prevent a computer virus or any form of system contamination from occurring. Classified information will only be processed on U.S. Government equipment, in secured work spaces, and handled in accordance with applicable directives.

f. Systems used for processing, handling or storing SCI information will be operated and secured in compliance with DIA Manual 50-4.

4. STANDARD FOR USE OF NON-REMOVABLE HARD DISK. Current policy does not prohibit the use of computers with non-removable hard disk drives when processing classified information. However, certain criteria must be met and adhered to when doing so:

a. If the facility is approved for open storage of classified information, there are no special

requirements.

b. If the facility is not approved for open storage of classified information, one of two procedures must be followed.

(1) The system must be secured in a safe or vault whenever not attended by cleared, authorized persons.

(2) A review of the hard disk directory must be accomplished prior to classified processing and again after the classified processing is completed.

c. If the option in paragraph 4.b.2 is implemented, the DAA must waive the requirement to classify the system and accept any residual risk that classified data might have been transferred onto the hard disk.

5. PROCEDURES FOR NON-REMOVABLE HARD DISK. The following are recommended procedures for classified processing on systems with non-removable hard disks. If the DAA accepts the risks and approves these procedures, he (DAA) may waive the requirement to classify the non-removable hard disk after classified processing. Implementation of these procedures should be in writing and the limits and sensitivity of information to be processed should be specified:

a. Prior to processing classified information, ensure that system defaults are set to write all information, including temporary files to the floppy drive.

b. Prior to processing classified information, dump a directory of the hard disk, including file sizes, dates written, and quantity of empty space to hardcopy.

c. While processing classified information, ensure that file names used do not duplicate the names of files on the hard disk. (The use of duplicate file names could result in an inadvertent write to the hard disk which might not be detectable by review of the directory dumps.).

d. Upon completion of the classified processing, dump a directory of the hard disk, including file sizes, dates written, and quantity of empty space to hard copy.

e. Compare the directory dumps made before and after the classified processing. If there are any differences, assume that classified information has been written to the hard disk and protect it appropriately.

f. If you are performing a period of classified processing to be followed by a period of unclassified processing, power the computer down for at least 30 seconds between the periods to purge Random Access Memory (RAM). Ensure that other memory buffers (i.e., printer buffers) are also purged.

g. In the event classified information is inadvertently written to a hard disk, the disk can be purged by overwriting with an approved product from NSA (refer to the EPL subset of the NSA prepared "Information Systems Security Products and Services Catalogue", available through subscription from GPO) or software authorized by DON. Refer to NAVSO Pub P5239-10 "ASSESSED PRODUCTS LIST" for DON approved computer security products that address this and other issues. The appropriate authority must then decide whether or not to remove the classification from the hard disk.

6. STANDARDS FOR FLOPPY DISKS. The following guidance is provided for 5 1/4 and 3 1/2 inch floppy diskettes:

a. All Classified diskettes will be color coded according to the highest classification of the information on them. The diskette jacket (the mylar plastic envelope which surrounds the magnetic medium) will be colored in its entirety according to the following color codes as depicted in DCID 3/14:

UNCLASSIFIED - BLACK, WHITE OR GRAY

SENSITIVE UNCLASSIFIED - GREEN

CONFIDENTIAL - BLUE

SECRET - RED

TOP SECRET - ORANGE

SCI - YELLOW

b. Classified information on floppy diskettes will be treated as working documents as defined in paragraph 10-8.1 of OPNAVINST 5510.1. However, paragraph 10-8.2 through 10-8.4 do not apply to documents on diskettes. Diskettes containing SCI working documents will be maintained in accordance with DoD C-5105.21-M-1.

c. SCI diskettes when assigned an SCI control number will be controlled, and accounted for by the Special Security Officer (SSO) in accordance with DOD C-5105.21-M-1.

d. Top Secret diskettes will be will be controlled, handled, and accounted for in accordance with OPNAVINST 5510.1. All other classifications of diskettes will be handled in accordance with OPNAVINST 5510.1 and local procedures.

e. Control numbers, dissemination control information (e.g., Restricted and NOFORN), and the owning organization, will be written on NON-SCI diskette jackets using an indelible ink marker. Ballpoint pens will not be used because they may damage the diskette. SCI diskettes will be marked in the same fashion except they will be also marked with the appropriate compartments and codewords.

f. Diskettes will not be downgraded, upgraded, or declassified with the exception of those containing SCI material. SCI material will be handled in accordance with DIAM 50-4.

g. Unclassified system diskettes and diskettes containing executable programs will be write-protected before they are inserted into a system which is processing classified information.

h. Diskettes received from vendors and sources outside the Marine Corps which are not color coded appropriately will be copied onto a properly colored diskette before use if authorized or feasible.

7. STANDARDS FOR OTHER REMOVABLE MEDIA. The following guidance is provided for other forms of removable magnetic media:

a. All other removable magnetic media (such as cassette tapes, removable hard disks, bubble memory boards) which contain classified data will be accounted for in accordance with the highest classification of data that they have contained per OPNAVINST 5510.1 (NON-SCI), DOD C5105.21-M-1 (SCI), and local procedures.

b. Magnetic media will be declassified or destroyed in accordance with CSC-STD-005 DOD Magnetic Remanence Security Guidelines, DOD C-5105.21-M.1, and NAVSUPP to DOD C-5105.21-M.1.

c. Media will be labeled with a color coded sticker label according to paragraph 6 above. Furthermore, a Data Descriptor label will be affixed to the media indicating the following:

CLASSIFICATION

CONTROL NUMBER

DISSEMINATION CONTROL INFORMATION (e.g., RESTRICTED or NOFORN)

OWNING ORGANIZATION

Use COMPARTMENTS/CODEWORDS, PHONE, CONTENT, and COMMENTS

where applicable

8. DISKETTE DESTRUCTION. The primary means of diskette destruction is incineration. Because not all organizations are permitted or have the facilities to destroy classified diskettes by incineration, the following alternative methods of destruction are authorized:

a. Overwrite all data bit locations as described in paragraph 5.3.1 of CSC-STD-005 DOD Magnetic Remanence Security Guidelines or reformat the diskette using a utility which overwrites all tracks and sectors. After overwriting, degauss the diskette using an NSA approved degausser (refer to the Degausser Products List (DPL) subset of the NSA prepared "Information Systems Security Products and Services Catalogue", available through subscription from GPO)).

b. Shred the diskette using a shredder authorized for classified information. The shredded pieces may be disposed of as unclassified waste. If the diskette cannot be shredded as a unit, remove the magnetic media from the colored envelope and shred the magnetic media.

c. Destruction of magnetic media containing SCI material will be conducted in accordance with DOD C-5105.21-M-1 and NAVSUPP to DOD C-5105.21-M-1.

9. REQUISITION OF COLOR CODED DISKETTES. Pre-labeled color coded diskettes are available to be ordered specifying "Marine Corps Color Coded Diskettes" from:

International Business Supplies (IBS), Incorporated

8730 Greenwood Place

Savage, Maryland 20763

Phone 1-800 458-7700 (Toll free)

(410) 880-4220 (Baltimore, Maryland area)

a. 5 1/4 inch diskette (360KB)

CENTECH 5.25 Flexible Disks (DS/DD/MS/UF)

Order: HR51D-S RED

HR51D-SCI YELLOW

HR51D-T ORANGE

HR51D-C BLUE

b. 5 1/4 inch diskette (1.2 MB)

CENTECH 5.25 Flexible Disks (DS/QD/96TPI/MS/UF/RH)

Order: HR5196D-S RED

HR5196D-SCI YELLOW

HR5196D-T ORANGE

HR5196D-C BLUE

c. 3 1/2 inch micro disks (720 KB)

KAO 3.5 Inch Disks (DS/DD/135TPI/MS/UF)

Order: MF2DD-KAORED-S

MF2DD-KAOYELLOW-SCI

MF2DD-KAORANGE-TS

MF2DD-KAOBLUE-C

MF2DD-KAOGREEN-SU

* d. Maximum individual order limit: 200 boxes (2000 diskettes)

e. Orders for comparable disks may be placed against other GSA contracts or open competitive procurement requests provided the quality of the recording media (Polyethylene terephthalate), diskette warranty (lifetime), and DCID 3/14 Pantone Matching System (PMS) printer ink colors are guaranteed to the government.

10. COLOR CODED MAGNETIC MEDIA LABELS. Labels (stickers) for removable magnetic media (for other than pre-labeled color coded diskettes) are available through the Marine Corps/Federal supply system (as applicable). Labels may be ordered using the following specifications:

a. "Magnetic Media Classification Label - CONFIDENTIAL", Standard Form (SF) 708, National Stock Number (NSN) 7540-01-207-5538, Unit of Issue: Pad of 300 labels.

b. "Magnetic Media Classification Label - SECRET", SF 707, NSN 7540-01-207-5537, Unit of Issue: Pad of 300 labels.

c. "Magnetic Media Classification Label - TOP SECRET", SF 706, NSN 7540-01-207-5536, Unit of Issue: Pad of 300 labels.

d. "Magnetic Media Classification Label - DATA DESCRIPTOR", SF 711, NSN 7540-01-207-5541, Unit of Issue: Pad of 300 labels.

e. "Magnetic Media Classification Label - SCI", NAVMC 11179, Stock Number (SN) 0000-00-006-9680, Unit of Issue: Pad of 50 labels.

f. "Magnetic Media Classification Label - SENSITIVE UNCLASSIFIED", NAVMC 11196, SN 0000-00-007-0100, pad of 50 Labels.

11. COLOR CODED SYSTEM ACCREDITATION LABELS. System accreditation will not become effective until a formal, dated, statement of accreditation has been issued by the DAA. The rectangular block on the accreditation label will reference the DAA's accreditation letter or interim authority to operate. Minimally, a system shall be accredited every 3 three years, regardless of changes. System accreditation labels (stickers) 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 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.

12. ORDERING OF DOCUMENTS. The following information concerning sources for ordering NSA/NCSC documents is provided:

a. INFORMATION SYSTEMS SECURITY PRODUCTS AND SERVICES

CATALOGUE, published by NSA on quarterly basis

Jan, Apr, July, Oct - Yearly Subscription \$54

Address to: Superintendent of Documents

US Government Printing Office

Washington, D.C. 20402

Phone Orders: (202) 783-3238 commercial

b. DOD 5200.28-STD "DOD TRUSTED COMPUTER SYSTEM EVALUATION
CRITERIA" (ORANGE BOOK)

No charge for single document

Address to: Director, National Computer Security Center

Attn: X71, (MRS KELLER)

Ft George G. Meade, Maryland 20755-6000

Phone Order: Single copies (410) 766-8729

c. NCSC-TG-025 Version 2 "A GUIDE TO UNDERSTANDING DATA
REMANENCE IN AUTOMATED INFORMATION SYSTEMS

No charge for document

Address/Phone: Same as 12.b above

d. NCSC-TG-005 Version 1 "TRUSTED NETWORK INTERPRETATION"

No charge for document

Address/Phone: Same as 12.b above

e. NCSC-TG-013 "RATING MAINTENANCE PHASE, PROGRAM DOCUMENT"

No charge for document

Address/Phone: same as 12.b above

f. CSC-STD-002-85 DOD "PASSWORD MANAGEMENT GUIDELINE"

No charge for document

Address/phone: same as 12.b above

g. CSC-STD-003-85 "COMPUTER SECURITY REQUIREMENTS-Guidance for applying the DOD TCSEC in specific Environments"

No charge for document

Address/phone: same as 12.b above

h. CSC-STD-004-85 "TECHNICAL RATIONALE behind implementing CSC-STD-003-85 Computer Security Requirements"

No charge for document

Address/phone: same as 12.b above

i. NCSC-TG-001 Version 2 "A Guide to Understanding AUDIT IN TRUSTED SYSTEMS"

No charge for document

Address/phone: same as 12.b above

j. NCSC-TG-003 Version 1 "A Guide to Understanding DISCRETIONARY ACCESS CONTROL in Trusted Systems"

No charge for document

Address/phone: same as 12.b above

k. NCSC-TG-004 Version 1 "GLOSSARY OF COMPUTER SECURITY TERMS"

No charge for document

Address/phone: same as 12.b above

l. NCSC-TG-006 Version 1 "A Guide to Understanding
CONFIGURATION MANAGEMENT in Trusted Systems"

No charge for document

Address/phone: same as 12.b above

m. NCSC-TG-007 Version 1 "A Guide to Understanding DESIGN DOCUMENTATION in
Trusted Systems"

No charge for document

Address/phone: same as 12.b above

n. NCSC-TG-008 Version 1 "A Guide to Understanding TRUSTED DISTRIBUTION in Trusted
Systems"

No charge for document

Address/phone: same as 12.b above

o. NCSC-TG-009 Version 1 "COMPUTER SECURITY SUBSYSTEM
INTERPRETATION of the TCSEC"

No charge for document

Address/phone: same as 12.b above

p. NCSC-TG-014 Version 1 "Guidelines for FORMAL VERIFICATION SYSTEMS"

No charge for document

Address/phone: same as 12.b above

q. NCSC-TG-015 Version 1 "A Guide to Understanding TRUSTED FACILITY
MANAGEMENT"

No charge for document

Address/phone: same as 12.b above

r. NCSC-TG-019 Version 2 "TRUSTED PRODUCT EVALUATION Questionnaire"

No charge for document

Address/phone: same as 12.b above

s. NCSC-TG-011 Version 1 "TRUSTED NETWORK INTERPRETATION
Environments Guideline"

No charge for document

Address/phone: same as 12.b above

t. NCSC-TG-002 Version 1 "TRUSTED PRODUCT EVALUATIONS,
A Guide for Vendors"

No charge for document

Address/phone: same as 12.b above

u. NCSC-TG-021 " Version 1 "TRUSTED DATABASE MANAGEMENT
SYSTEM INTERPRETATION of Trusted Computer System Evaluation Criteria"

No charge for document

Address/phone: same as 12.b above

v. NCSC-TG-017 Version 1 "A guide to Understanding IDENTIFICATION And
AUTHENTICATION in Trusted Systems"

No charge for document

Address/phone: same as 12.b above

w. NCSC-TG-018 Version 1 "A Guide to Understanding OBJECT REUSE in Trusted Systems"

No charge for document

Address/phone: same as 12.b above

x. NCSC-TG-022 Version 1 "A Guide to Understanding TRUSTED RECOVERY in Trusted Systems"

No charge for document

Address/phone: same as 12.b above

y. NCSC-TG-026 Version 1 "A Guide to Writing the SECURITY FEATURES USER'S GUIDE for Trusted Systems"

No charge for document

Address/phone: same as 12.b above

z. NCSC-TG-027 Version 1 "A Guide to Understanding INFORMATION SYSTEM SECURITY OFFICER Responsibilities for Automated Information Systems"

No charge for document

Address/phone: same as 12.b above

aa. NCSC-TG-028 Version 1 "Assessing CONTROLLED ACCESS PROTECTION (CAP)"

No charge for document

address/phone: same as 12.b above

bb. NCSC-TG-016 Version 1 "GUIDELINES for writing TRUSTED FACILITY MANUALS"

No charge for document

address/phone: same as 12.b above

cc. NCSC-TG-010 Version 1, "A Guide to Understanding SECURITY MODELING in Trusted Systems"

No charge for document

address/phone: same as 12.b above

dd. NCSC-TG-024 Volume 1/4, Version 1 "A Guide to Procurement of Trusted Systems: AN INTRODUCTION TO PROCUREMENT INITIATORS ON COMPUTER SECURITY REQUIREMENTS"

No charge for document

address/phone: same as 12.b above

ee. NCSC-TG-024 Volume 2/4, version 1,"A Guide to Procurement of Trusted Systems: LANGUAGE FOR RFP SPECIFICATIONS AND STATEMENTS OF WORK-AN AID TO PROCUREMENT INITIATORS"

No charge for document

address/phone: same as 12.b above

ff. NCSC-TG-023 Version 1, "A Guide to Understanding SECURITY TESTING AND TEST DOCUMENTATION"

No charge for document

address/phone: same as 12.b above

gg. NCSC-TG-024 Volume 3/4, version 1, "A Guide to Procurement of Trusted Systems: COMPUTER SECURITY CONTRACT DATA REQUIREMENTS LIST AND DATA ITEM DESCRIPTION TUTORIAL"

No charge for document

address/phone: same as 12.b above

hh. NCSC-TG-029 Version 1, "INTRODUCTION TO CERTIFICATION AND ACCREDITATION"

No charge for document

address/phone: same as 12.b above

ii. NCSC TECHNICAL REPORT-002, "USE OF THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC) FOR COMPLEX, EVOLVING, MULTIPOLICY SYSTEMS", Library No. S-241,321

No charge for document

address/phone: same as 12.b above

jj. NCSC TECHNICAL REPORT-003, "TURNING MULTIPLE EVALUATED PRODUCTS INTO TRUSTED SYSTEMS", Library No. S-241,353

No charge for document

address/phone: same as 12.b above

kk. NCSC TECHNICAL REPORT-004, "A Guide To PROCUREMENT OF SINGLE AND CONNECTED SYSTEMS", Library No. S-241, 359

No charge for document

address/phone: same as 12.b above

ll. NCSC-TG-020-A Version 1, "TRUSTED UNIX WORKING GROUP (TRISOX) RATIONALE FOR SELECTING ACCESS CONTROL LIST FEATURES FOR THE UNIX SYSTEM"

No charge for document

address/phone: same as 12.b above

mm. NCSC-TG-030 Version 1, "A Guide To Understanding COVERT

CHANNEL ANALYSIS Of Trusted Systems

Appendix D

COMPUTER LOG-ON WARNING SCREEN

1. The Computer Fraud and Abuse Act of 1986 (P.L. 99-474) requires in part that all government computers have a warning screen message in place to make users of federal computer systems aware of their responsibilities with respect to the use of government computers.

2. During the initial boot of a computer system, and before any user can perform any work, the following message will appear on the screen (monitor) in a fashion that requires the user to take an overt action to clear the screen. That is, the message must not automatically scroll off the screen. The user must hit a key to clear the message from the screen. The message will read as follows:

"USE OF THIS OR ANY OTHER DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES This is a DOD interest computer system. All DOD interest computer systems and related equipment are for communication, transmission, processing, and storage of official U.S. Government or other authorized information only. These systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices, to prevent unauthorized use and violations of statutes or security regulations, to deter criminal activity, and for other similar purposes. Any user should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy. If monitoring of this or any other DOD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DOD interest computer system reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DOD interest computer systems are subject to appropriate disciplinary action.

"POWER OFF SYSTEM TO CANCEL UNAUTHORIZED USE"

3. Listed below are PC installation guidelines for the warning screen. Both methods will display a warning screen every time the system is rebooted. All of the instructions below should be executed after loading the warning message to a file called "WARNING.ASC" onto a scratch diskette.

The simplest way to install the warning screen is to call it from the AUTOEXEC.BAT file. The procedures below will work with MS-DOS.

Installation for FLOPPY-DISK based systems:

a. Make sure DOS disk contains the files: COMMAND.COM

b. Boot up system with DOS disk in drive A:

c. If you already have an AUTOEXEC.BAT file, then insert the following FOUR (4) commands at the beginning of the file (i.e., these four commands MUST be the 1st four lines in the file):

ECHO OFF

CLS

TYPE WARNING.ASC

PAUSE

d. If you do not already have an AUTOEXEC.BAT, then:

Key in "COPY CON AUTOEXEC.BAT"

Key in the following FIVE (5) commands, pressing RETURN/ENTER after each command:

ECHO OFF

CLS

TYPE WARNING.ASC

PAUSE

ECHO ON

e. Press "Ctrl" and "Z" simultaneously, and press RETURN/ENTER key.

f. Put the WARNING diskette in drive B:

g. Key in the command "COPY B:WARNING.ASC A:

Note: Repeat this procedure for any disk that you use to boot your system.

Installation for HARD-DISK based systems:

The following installation must be executed from within the directory which contains your COMMAND.COM file (i.e., normally your "root" directory). The AUTOEXEC.BAT and WARNING.ASC files MUST be in the same directory.

a. Boot-up your system.

b. If you already have an AUTOEXEC.BAT file then insert the following FOUR (4) commands at the beginning of the file (i.e., these four commands MUST be the 1st four lines in the file):

ECHO OFF

CLS

TYPE WARNING.ASC

PAUSE

c. If you do not already have an AUTOEXEC.BAT, then:

Key in "COPY CON AUTOEXEC.BAT"

Key in the following FIVE (5) commands, pressing RETURN/ENTER after each command:

ECHO OFF

CLS

TYPE WARNING.ASC

PAUSE

ECHO ON

d. Press "Ctrl" and "Z" simultaneously, and press RETURN/ENTER key.

e. Put the WARNING diskette in drive A:

f. Key in the command "COPY A:WARNING.ASC C:"

Appendix E

SENSITIVE UNCLASSIFIED INFORMATION

1. INTRODUCTION. Computer systems handling Sensitive Unclassified information must protect information equal to the level of risk and magnitude of harm that could result from disclosure, loss, misuse, alteration or destruction. In this regard, The Computer Security Act of 1987 (P.L. 100-235), requires U.S. agencies to identify each computer system which contains Sensitive Unclassified information and to provide for the security and privacy of each such system.

2. SENSITIVE UNCLASSIFIED. The roles and responsibilities for protecting Sensitive Unclassified information in systems are often similar to those required for protecting classified systems. The primary difference is in the sensitivity of the data, not in the requirement for protection. The term includes records about individuals requiring protection under the Privacy Act, proprietary data, information not releasable under the Freedom of Information Act, and DOD and Marine Corps data that affects the mission.

3. IDENTIFYING SENSITIVE UNCLASSIFIED DATA. Examples of different type and categories of Sensitive Unclassified data:

a. Personal Data. The Privacy Act of 1974 prohibits unauthorized access to records containing personal data (information about an individual). The Privacy Act requires that appropriate administrative, technical, and physical safeguards be used to ensure record security and confidentiality. This includes all personnel records, whether in the information system maintained in personnel offices or in a separate information system used by the supervisor. Examples include:

(1) Medical Records.

(2) Individual financial information.

(3) Manpower and personnel records.

(4) Training records.

b. Privileged Data. Functional users regulate this category. Examples include:

- (1) Chaplain records.
- (2) Judge Advocate records.
- (3) Internal organization management records.
- (4) Safety records.

c. Proprietary Data. This includes data that are the exclusive property of an individual or civilian corporation and is on loan to the Marine Corps through a licensing agreement or made available to the government. Functional users regulate this category of data. An example is copyrighted material.

d. Other Types of Sensitive Unclassified Data. Examples of other data that are considered Sensitive Unclassified and require appropriate protection:

- (1) Logistics records.
- (2) Procurement data.
- (3) Financial data.
- (4) Source selection sensitive data.
- (5) Investigative data.
- (6) Automated decision-making aids (models).
- (7) Maintenance records.
- (8) Auditor reports.
- (9) Essential elements of friendly information (EEFI)
- (10) FOUO data.
- (11) Critical technologies.
- (12) Scientific and technical data.
- (13) Unit mobility or deployment information.
- (14) War reserve material data.

e. Aggregated Data. Information that is unclassified individually may require classification when combined or associated with other unclassified information. The sensitivity of aggregated data elements can require a higher level of protection than data elements standing alone. The Manpower Mobilization Planning System (MMPS) is an example of aggregated data identified and currently regulated as classified information. Functional managers should:

(1) Address aggregation of data early in the life cycle of automated systems.

(2) Use aggregated data to justify higher levels of security protection.

(3) Document aggregation resulting in data changing from unclassified to classified in the security classification guide.

(4) Document aggregation resulting in higher sensitivity in security plans and other security documents developed in the life cycle.

Note: In today's multi-use environment, a user can access multiple systems and databases via a LAN and in turn, download, merge and sort data from various sources on an intelligent terminal. The compromise of security is much more likely in this scenario. Security considerations for Local and Wide Area Networks is contained in IRM-5239-04.

4. Documentation Requirements. Identify the authority source used to determine level of sensitivity and document it in the risk assessment (Appendix B lists reference documents to help determine protection authority requirements). The analysis supporting the sensitivity levels, other than those identified above, must be kept with the risk assessment documentation to ensure the maintenance of prescribed minimum security requirements.

5. Minimum Security Requirements. The following security safeguards are mandatory for computer systems used to process Sensitive Unclassified information. These security requirements can be fulfilled through a TCB or a combination of physical, information, communications, personnel, and procedural security measures including various security modes of operation. Minimum requirements are:

a. Appropriate marking.

b. Access control over processes, files, segments, and devices.

c. Identification and authentication (user ID and password).

d. Audit (system and file access).

e. Protection of systems as a resource and protection against Fraud, waste and abuse.

6. LCM of Sensitive Unclassified Systems. A risk assessment dictates the level of protection required for a specific system. Life-cycle management applies to all systems.

7. Security Modes of Operation. Systems processing unclassified may operate in several modes depending on system capabilities and security requirements. Modes of operation can be combined with other security disciplines to ensure a proper level of security.

Appendix F

SECURITY MODES OF OPERATION

1. INTRODUCTION. Successful implementation of minimum security requirements on a computer system requires consideration of protection mechanisms inherent in the system. The security mode of operation depends directly on the adequacy and reliability of internal system hardware and software controls. When controls are weak or nonexistent, external control measures and the proposed mode of operation must be adjusted until an acceptable security posture is obtained.

2. MODES OF OPERATION. An evaluation of information, user clearance and need-to-know, and proposed or in place protection mechanisms form the basis for selecting the appropriate security mode of operation.

a. Dedicated Security Mode. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

b. System High Security Mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

c. Multilevel Security Mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS. This mode is also referred as MLS.

d. Partitioned Security Mode. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. This security mode encompasses the compartmented mode defined in DCID No. 1/16.

e. Periods Processing. A manner of operating an AIS in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during the period.

3. MINIMUM REQUIREMENTS. Each system, regardless of mode of operation, must provide protection in the areas described below. Conditions to consider include the mission; environment; volume, frequency, sensitivity, and criticality of processing; mode of operation; system configuration; and hardware and software functional capabilities.

a. Individual User Accountability. User identity must be positively established. User access and activity in the system (material accessed and actions taken) must be controlled and open to scrutiny. Generally, this requirement is met by applying a combination of administrative procedures and hardware and software controls. The degree of reliance on hardware and software controls ranges from negligible in the dedicated security mode to extensive in the multilevel security mode. An automated audit trail should show data collected from accesses made to system files and all unauthorized access attempts.

b. Physical Control. Measures must insure external protection against unauthorized access to the main computer location, to the system from remote terminals, and to data storage media.

c. System stability. Computer components should operate automatically to administratively detect and report system hardware and software malfunctions in time to prevent unauthorized disclosure.

d. Data Integrity. Each data base, file, or data set must have an origin, use, and a defined set of access controls. Information classification, sensitivity, user clearance, and established need-to-know should be the basis for access controls.

e. System Reliability. In system high, controlled, multilevel ~~and~~ multiuser security modes, the system must operate so users can access only authorized information.

f. Telecommunications. Plan integral telecommunications systems, considering all elements of COMSEC and baseline during the conceptual phase and throughout the system life cycle.

g. Classified Information. Machine-mark and protect classified information according to its classification.

h. Sensitive Unclassified Information. Protect Sensitive Unclassified information the system processes equal to the level of risk that could result from disclosure, loss, misuse, alteration or destruction.

4. TRUSTED COMPUTER SYSTEMS EVALUATION CRITERIA. When acquiring a system to process either classified or Sensitive Unclassified information, adequate system internal security control mechanisms are essential to protect the system and data. Table F-1

identifies the level of trust (as defined in DOD Standard 5200.28-STD) needed to protect each level of classified or Sensitive Unclassified data in a particular mode of operation. Criticality may require a higher level of trust than that reached from the intersection of clearance and sensitivity. Presently, there are few systems meeting the established criteria. Until such systems

become widely available, a combination of physical, personnel, administrative, procedural, firmware, and hardware and software controls are necessary to achieve an overall protection comparable to the identified criteria level. The DAA determines what constitutes an adequate level of overall protection for the system and data.

DATA SENSITIVITY

Without Categories

MINIMUM

USER CLEARANCE

Sensitive Top

Unclas Unclas Confidential SecreSecret

Uncleared N/A B1 B2 B3 A1

or Not

Authorized

Uncleared N/A C2 B1 B2 A1

but Authorized

Access to

SensitiveUncl

Confidential N/A C2C2 B1 B3

Secret N/A C2C2 C2 B2

Top Secret N/A C2C2 C2 C2

(Current BI)

Top Secret N/A C2C2 C2 C2

(Current SBI)

One Category N/A C2C2 C2 C2

Multiple N/A C2C2 C2 C2

Categories

Table F-1

Trusted Systems Criteria

(Based on DOD Standard 5200.28-STD)

DATA SENSITIVITY

With Categories

MINIMUM

USER CLEARANCE

Sensitive Top

Unclas Unclas Confidential Secret

Uncleared N/A N/A N/A N/A N/A

or Not

Authorized

Uncleared N/A C2 B2 B3 A1

but Authorized

Access to

Sensitive Uncl

Confidential N/A C2 B1 B2 A1

Secret N/A C2 C2 B1 B3

Top Secret N/A C2 C2 C2 B2

(Current BI)

Top Secret N/A C2C2 C2 B1

(Current SBI)

One Category N/A C2C2 C2 C2

Multiple N/A C2C2 C2 C2

Categories

Table F-2

Trusted Systems Criteria

(Based on DOD Standard 5200.28-STD)

Appendix G

TEMPEST COUNTERMEASURE REVIEW (TCR) (U)

1. Prior to processing classified data (except those systems located on military bases within the U.S. that process data classified no higher than SECRET), a TEMPEST Countermeasure Review shall be forwarded to NISE EAST with a copy to CO, NAVELEXSECCEN, CMC (Code CSBT), and other commands as appropriate. The following information is required for a TCR as indicated in OPNAVINST C5510.93:

a. Identification of both the command possessing the CLIPS and responsible for its security, and the command submitting the TCR. Provide the NTP-3 short title for both, and the name and phone number of points-of-contact at both.

b. General description of data being processed (e.g., messages, radar/sonar, telemetry).

c. Listing and description of the equipment and systems, including individual system component nomenclature and model numbers of stand-alone equipment which will process classified information. Include statement concerning TEMPEST posture of system/equipment (i.e., off-the-shelf, built or modified to meet NACSIM 5100, EZN, etc.). Include the total volume of data handled and the period over which such a volume is handled. Volume should be in terms of the type of processing done (e.g. "messages" for a communication center, "pages" for a printing facility or "screens" if the processing is done primarily on video terminals). Additionally, a breakout, in percentages, of the volume at each classification level should be made and a listing provided of types of compartmented data, if any, that are processed. Identify specific equipment deleted, added or relocated since last Instrumented TEMPEST Survey (ITS) of this system.

d. Indicate if the equipment will be installed within a shielded enclosure which provides a minimum of 60 dB of attenuation. If so provide the following:

(1) Manufacturer of enclosure.

(2) Date installed.

(6) Location of CLIPS showing the minimum distance, in meters, from CLIPS components to the boundary of the CS. Use a separate sheet to key all CLIPS to the listing provided under paragraph 1.c, above.

f. If the specific CLIPS has been previously surveyed, provide the result, date and reference of last ITS for each CLIPS together with a listing of the specific equipment or systems deleted, added or relocated since last ITS. If the system failed the previous survey, such a statement will make the TCR classified.

g. Statement as to whether CLIPS was installed following appropriate RED/BLACK criteria. Statement of specific CM determined to be necessary during evaluation and whether CM was met. If CM4 was called out and met, the command should state here "Based upon the fact all components which process classified information are installed properly, we will consider this installation an acceptable risk unless otherwise notified".

h. Description of power source (i.e., commercial, government, filtered, unfiltered, motor generator, etc.).

i. Will signal lines carrying unencrypted classified/compartmented information be routed into areas of lower classification/compartmentation or into uncontrolled areas? If so, describe TEMPEST and physical security protective measures. Will compartmented data be transmitted outside the compartmented area? If so, identify organization, location, building, and room number of distant end for each circuit.

j. For compartmented processors identify lines, cables, and other metallic conductors which leave the CS, including telephone, power, signal, and alarm lines, pipes, air conditioning ducts, etc.

k. For compartmented processors indicate the location of telephone instruments, telephone line filters, power line filters, signal ground points, etc. on the drawings provided under item "e." above.

l. For compartmented processors, are telephone lines:

(1) Shielded? _____ YES _____ NO.

(2) In conduit? YES NO.

(3) Filtered? YES NO. If Yes, are filters grounded within
the controlled space? YES NO.

(4) Distributed separately from all classified signal lines? YES
 NO.

(5) A minimum of one meter from any CLIPS? YES NO.

2. Remarks. Include any amplifying information that could assist in determining hazard probabilities and subsequent TEMPEST survey schedule.

Appendix H

TECHNICAL VULNERABILITY REPORT (DoD)

Reporting Format. The following format should be used for reporting technical vulnerabilities in hardware, firmware, or software as required by DoD Instruction 5215.2.

Vulnerability Report

Classification markings

I. Required Information:

A. Report date.

B. Contact.

1. Name.

2. Organization.

3. Mailing and message address.

4. AUTOVON and commercial telephone number.

5. Position and title.

C. Hardware and Software.

1. Source: Military or commercial.

2. List hardware and system configuration.

3. Software description.

a. Operating System (including release number #)

b. Any unique attributes such as locally modified, special properties, and so forth.

II. Executive Summary of Vulnerability.

Describe the nature and the effect of the technical vulnerability in general terms.

III. Description of Technical Vulnerability:

A. This should be a scenario that describes the specific conditions to demonstrate the vulnerability. The description must sufficiently describe the conditions so that the flaw can be repeated without further information. This scenario may include source or object code.

B. Describe the specific impact or effect of the technical vulnerability in terms of the following categories (cite specific examples).

1. Denial of service.

2. Alteration of information.

3. Compromise.

4. Other.

C. Indicate if the affected vendor has been notified.

IV. Suggested Fixes.

Describe codes or procedures that may reduce the impact of the defined technical vulnerability.

V. Additional Information:

A. System specifics:

1. Location.

2. Owner.

3. Network connections.

4. Security attributes.

B. System use and highest classification of data on system.

C. Additional clarifying information.

COMMENTS/REVISION

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: CG MCCDC

Requirements Division (C44)

3300 Russell Road

Quantico, VA 22134-5001