IRM-5239-13

U.S. Marine Corps

SYSTEM SECURITY PLAN

PCN 186 523913 00

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

IN REPLY REFER TO
5239/13
CCIS-31
30 APR 1991

From: Commandant of the Marine Corps

Subj: SYSTEM SECURITY PLAN

Ref: (a) P.L. 100-235, Computer Security Act of 1987
(b) DODD 5200.28
(c) MCO P5231.1B
(d) MCO 5271.1

Encl: (1) IRM-5239-13

1. PURPOSE. To provide guidance, instructions and format on the development of a System Security Plan as required by references (a) through (c).

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

3. APPLICABILITY. The guidance contained in this publication is applicable to all Marine Corps and contractor personnel. The System Security Plan (SSP) is required by reference (a) to provide a basic overview of the security and privacy requirements for all computer systems that process or store Sensitive Unclassified information. Life Cycle Management for Automated Information Systems (LCM-AIS) requires developers of AISs to incorporate the SSP throughout the AIS development (reference (c)). Excluded from the scope of this publication are classified information and information embedded in tactical/combat weapons systems. 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. Accountability. A copy of the SSP and all supporting documentation shall be retained by the responsible organization as a permanent record for future reference on computer security reaccreditation reviews, internal control reviews, vulnerability assessments, or general audit purposes.

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

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

5239/10
CCIS-31

Subj: INTEGRATION SUPPORT CONTRACT USER'S GUIDE

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

G. L. MCKAY
by direction

DISTRIBUTION: 186 523913 00

Copy to: 8145001

UNITED STATES MARINE CORPS

Information Resources Management (IRM) Standards
and Guidelines Program

SYSTEM SECURITY PLAN
IRM-5239-13

Enclosure (1)

(This page intentionally left bank)

RECORD OF CHANGES

Log completed change action as indicated.

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

(This page intentionally left blank)

PUBLICATION TABLE OF CONTENTS

		Paragraph	Page
	Chapter 1		
	GENERAL		
Section 1.	INTRODUCTION	1.1.	1-3
Section 2.	PURPOSE	1.2.	1-3
Section 3.	GENERAL INFORMATION	1.3.	1-3
Section 4.	MAJOR APPLICATION(AIS) VS GENERAL SUPPORT SYSTEMS (GSS)	1.4.	1-4
Section 5.	THE SSP COMPONENTS	1.5.	1-7
Section 6.	REFERENCES AND DEFINITIONS	1.6.	1-7
Section 7.	SSP BLANK WORKSHEETS	1.7.	1-7
	Chapter 2		
	BASIC SYSTEM IDENTIFICATION		
Section 1.	GENERAL	2.1.	2-3
Section 2.	RESPONSIBLE ORGANIZATION (1a)	2.2.	2-3
Section 3.	SYSTEM NAME/TITLE (1b)	2.3.	2-3
Section 4.	SYSTEM CATEGORY (1c)	2.4.	2-8
Section 5.	LOCATION INFORMATION (1d)	2.5.	2-8
Section 6.	SYSTEM OPERATIONAL STATUS (1e)	2.6.	2-8
Section 7.	GENERAL DESCRIPTION/PURPOSE (1f)	2.7.	2-9
Section 8.	SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS (1g)	2.8.	2-9
Section 9.	INFORMATION CONTACT(S) (1h)	2.9.	2-9
	Chapter 3		
	SENSITIVITY OF INFORMATION HANDLED		
Section 1.	GENERAL	3.1.	3-3
Section 2.	MID-RANGE INFORMATION SYSTEMS PLAN (MRISP)	3.2.	3-3
Section 3.	GENERAL DESCRIPTION OF INFORMATION SENSITIVITY (2a)	3.3.	3-3
Section 4.	SYSTEM CLASSIFICATION (2b)	3.4.	3-7
Section 5.	APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM (2c)	3.5.	3-7
Section 6.	PROTECTION REQUIREMENT (2d)	3.6.	3-7
Section 7.	LEVEL OF PROTECTION (2e)	3.7.	3-8

Chapter 4

SYSTEM SECURITY MEASURES

Section 1.	GENERAL	4.1.	4-3
Section 2.	RISK MANAGEMENT	4.2.	4-3
Section 3.	SECURITY CONTROL MEASURES - MAJOR APPLICATIONS(AIS) (3c)	4.3.	4-6
Section 4.	SECURITY CONTROL MEASURES - GENERAL SUPPORT SYSTEMS (GSS) (3c)	4.4.	4-11
Section 5.	SUPPORTING DOCUMENTATION (3d)	4.5.	4-15
Section 6.	SECURITY CONTROL MEASURE STATUS (3e)	4.6.	4-15
Section 8.	ADDITIONAL COMMENTS (4)	4.8.	4-16

APPENDICES

A.	PUBLIC LAW 100-235, COMPUTER SECURITY ACT OF 1987	A-1
B.	REFERENCES	B-1
C.	TERMS AND DEFINITIONS	C-1
D.	CROSS REFERENCES TO EXISTING SECURITY PUBLICATIONS	D-1
E.	SSP BLANK WORKSHEETS	E-1

LIST OF FIGURES

Figure		Page
1-01	Common Computer Systems and Responsible Organization/Individuals	1-5
1-02	Major Applications(AIS)	1-6
1-03	General Support Systems	1-6
1-04	Correlation Between the SSP and This Technical Publication	1-7
2-01	Completed Basic System Identification (AIS)	2-4
	Completed Basic System Identification (GSS)	2-5
	Continuation of Basic System Identification (AIS)	2-6
	Continuation of Basic System Identification (GSS)	2-7
2-02	Responsible Organization	2-8
2-03	System Name/Title	2-8
2-04	General Description/Purpose	2-9
2-05	System Environment and Special Considerations	2-10
2-06	Information Contact(s)	2-10
3-01	Completed Sensitivity of Information Handled (AIS)	3-4
	Completed Sensitivity of Information Handled (GSS)	3-5
3-02	Privacy Data Codes	3-6
3-03	National Interest Data Codes	3-6
3-04	Information Requiring Confidentiality	3-7
3-05	Examples of Systems Requiring Integrity Protection	3-8
3-06	Examples of Systems Requiring Availability Protection	3-8
3-07	MRISP Entry for Protection Requirement	3-9
4-01	Completed System Security Measures (AIS)	4-4
	Continued System Security Measures (AIS)	4-5
	Completed System Security Measures (GSS)	4-6
4-02	Example of Security Control Measures Status	4-15

(This page intentionally left blank)

Chapter Table of Contents

Chapter 1

GENERAL

	Paragraph	Page
Section 1. INTRODUCTION	1.1.	1-3
Background	1.1.1.	1-3
Section 2. PURPOSE	1.2.	1-3
Section 3. GENERAL INFORMATION	1.3.	1-3
Use of This Technical Publication	1.3.1.	1-3
What is a Sensitive Unclassified Computer System?	1.3.2.	1-4
Who is Responsible for the SSP?	1.3.3.	1-4
SSP Requirements and Functions	1.3.4.	1-4
Section 4. MAJOR APPLICATIONS(AIS) VS GENERAL SUPPORT SYSTEMS(GSS)	1.4.	1-4
Major Application(AIS)	1.4.1.	1-4
General Support Systems(GSS)	1.4.2.	1-6
Section 5. THE SSP COMPONENTS	1.5.	1-7
Section 6. REFERENCES AND DEFINITIONS	1.6.	1-7
Section 7. SSP BLANK WORKSHEETS	1.7.	1-7

(This page intentionally left blank)

Chapter 1

GENERAL

1.1. INTRODUCTION

1.1.1. Background. The Computer Security Act of 1987, Public Law 100-235, mandates that Federal agencies implement security guidelines and standards and provide periodic training to all persons involved with Federal computer systems containing Sensitive Unclassified information. It also requires that all Federal computer systems containing Sensitive Unclassified information implement and maintain system security plans which are the main focus of this publication. Every Marine Corps computer system containing Sensitive Unclassified information is required to have a System Security Plan (SSP). (The Computer Security Act is contained in Appendix A.)

1.2. PURPOSE. The SSP is the documenting tool used to ensure that the requirements mandated in the Computer Security Act of 1987 are being implemented and adhered to. An SSP requires that every organization/individual responsible for Sensitive Unclassified computer system(s) conduct an appropriate review and analysis, (as outlined in the following chapters of this document), not only to identify the risks and vulnerabilities that might bring harm to the data but to provide the necessary protective measures as well. The SSP provides a structured methodology to follow and to help prevent potential problems from escalating. The SSP will also assist in such areas as system accreditation, Life Cycle Management for AISs, accountability of resources, identify training requirements, and information/status reporting.

1.3. GENERAL INFORMATION

1.3.1. Use of This Technical Publication. This technical publication was designed to assist Marine Corps computer users in the preparation of the SSP. The SSP is modeled after OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Unclassified Information. The examples provided throughout this document are intended to assist the SSP preparer in understanding what type of entry is expected or what action must be done. This publication provides only the foundation and skeletal outline for completing the SSP. Simply "filling in the appropriate blanks" will not be acceptable. The SSP represents what actions have been taken; what measures are in place; what procedures are being implemented; as well as the required documents that have been created and maintained in order to fulfil the security requirements. "Common sense and logic" are key factors in completing the SSP and in creating a living and useful plan that is intended to protect the information processed and stored on the computer systems.

1.3.2. What is a Sensitive Unclassified Computer System? A Sensitive Unclassified computer system is one that processes or contains Sensitive Unclassified information which the loss, misuse, or unauthorized access to, or modification of might adversely affect U.S. National interest, the conduct of DoD programs, or the privacy of DoD personnel. Most Marine Corps computer systems process information of this type. Systems that process only unclassified information, (data safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse), may also have an SSP.

1.3.3. Who is Responsible for the SSP? The SSP should be completed by the responsible organization for the computer system. The SSP has divided all computer systems into either Major Application(AIS) or General Support Systems. The responsible organization for a Major Application(AIS) is the staff agency whose mission includes the management responsibility for a specific functional area such as personnel, intelligence, operations, logistics, aviation or fiscal. The Functional Manager for the Major Application(AIS) is responsible for completing the SSP. The responsible organization for a General Support System is the organization that has physical custody of the General Support System. It is up to that organization to designate the SSP preparer, such as the Computer System Security Officer (CSSO), or a Terminal Area Security Officer (TASO).

1.3.4. SSP Requirements and Functions. The responsible organization is required to review the SSP annually to ensure that all information is current. The SSP must be updated any time there is a significant change to the computer system, environment or processing mode. The SSP is to be maintained as a permanent record and to be used for system accreditation and/or reaccreditation, internal reviews, or general audit purposes. The responsible organization should take appropriate time to become familiar with this technical publication in order to gain a complete understanding of what is expected. Figure 1-01 contains scenarios of the common computer systems found throughout the Marine Corps that would require an SSP.

1.4 MAJOR APPLICATIONS(AIS) VS GENERAL SUPPORT SYSTEMS(GSS)

1.4.1. Major Application(AIS). A Major Application(AIS) is a combination of information, computer, telecommunications resources and other information technology, and personnel resources which collects, records, processes, stores, communicates, retrieves and displays information. For the purpose of this technical publication, a Major Application(AIS) is also one that performs clearly defined functions for which there are readily identifiable security considerations and needs as defined in MCO P5231.1, LIFE CYCLE MANAGEMENT FOR AUTOMATED INFORMATION SYSTEMS (LCM-AIS) PROJECTS (LCM-AIS PROJECTS). A Major Application(AIS) must coincide with the security requirements stated in the LCM-AIS Order. Functional Managers

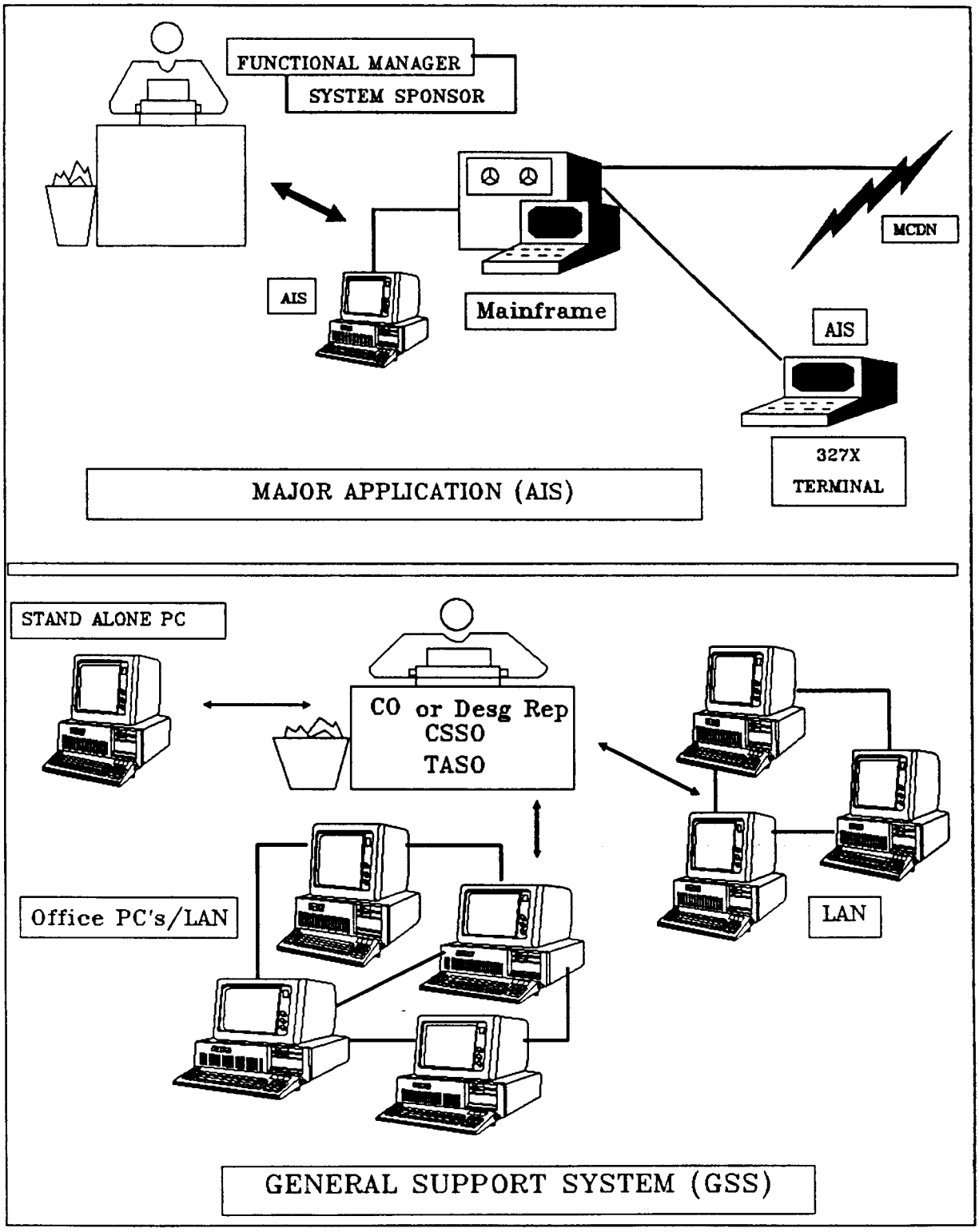

FIGURE 1-01
Common Computer Systems and Responsible Organization/Individuals

will be the only responsible organization completing the SSP for Major Applications(AIS). This includes all Class I systems and most of Class II systems. The SSP for Class III systems is the responsibility of the Federal Agency or organization (i.e. DoD) sponsoring the Major Application(AIS). Figure 1-02 contains examples of Major Applications(AIS) and their responsible organization.

Class I	MIMMS (I&L)
Class II	GUARDS (I&L)
Class III	DEERS (DoD)

FIGURE 1-02
Major Applications(AIS)

1.4.2. General Support Systems (GSS). General Support Systems are those systems comprised of hardware and software that provide general small computers or network support for a variety of user(s) and applications. GSS are utility oriented systems that can be thought of as tools used in the maintenance and support of day-to-day activities. A GSS can include word processing systems, commercial software packages and locally generated applications that assist the user in daily tasks that run on small computers. Figure 1-03 contains examples of General Support Systems (GSS).

HQMC LAN
Local Office LAN
Personnel Recall Roster System
Quantico Disbursing Office PC Cluster
Standalone PC

FIGURE 1-03
General Support Systems (GSS)

Since there are so many GSS throughout the Marine Corps that perform similar tasks with similar types of information, it would be a logical alternative to require one SSP for a group of these computer systems provided they share the following criteria:

- Located in close proximity (Office cluster)
- 2 to 25 Small Computers
- Same classification of data
- Similar software packages (wordprocessing, database, spreadsheet)
- Similar hardware configuration

NOTE: A computer system can only be reported once. For example, if a computer system is part of a LAN and an office cluster, the

SSP preparer for the LAN will only **reference** the computer system; whereas, the SSP preparer for the office cluster will **report** the computer system (including the LAN server) since they are accountable for the computer system. The LAN SSP would focus on the server and the physical addresses of the devices attached to the LAN and concentrate on the risks and vulnerabilities as they apply to the entire LAN from the server's standpoint. Computers attached to the LAN server, but not included in its SSP because they are in a different location or another unique situation, require their own SSPs, in which the LAN server would be referenced.

1.5. THE SSP COMPONENTS. There are three components to every SSP. Each SSP component has several blocks that require action either by checking an appropriate box or inserting a response. Figure 1-04 is a description of how the remaining chapters of this document correspond to each SSP Component.

Chapter 2 - Basic System Identification (The who, what, where, when, and why of the computer system)

Chapter 3 - Sensitivity of Information (The impact and reasons why the information must be safeguarded)

Chapter 4 - Security Measures (Actions taken to ensure the information is being safeguarded)

FIGURE 1-04
Correlation Between the SSP and this Technical Publication

1.6. REFERENCES AND DEFINITIONS. A list of references is contained in Appendix B. A list of terms and corresponding definitions is provided in Appendix C.

1.7. SSP BLANK WORKSHEETS. A System Security Plan (blank sheets) for Major Applications(AIS) and for General Support Systems are located at the end of this document for your use.

(This page left intentionally blank)

Chapter Table of Contents

Chapter 2

BASIC SYSTEM IDENTIFICATION

		Paragraph	Page
Section 1.	GENERAL	2.1.	2-3
Section 2.	RESPONSIBLE ORGANIZATION (1a)	2.2.	2-3
	Major Application(AIS)	2.2.1.	2-3
	General Support System (GSS)	2.2.2.	2-3
Section 3.	SYSTEM NAME/TITLE (1b)	2.3.	2-3
Section 4.	SYSTEM CATEGORY (1c)	2.4.	2-8
Section 5.	LOCATION INFORMATION (1d)	2.5.	2-8
	Major Application (AIS)	2.5.1.	2-8
	GSS	2.5.2.	2-8
Section 6.	SYSTEM OPERATIONAL STATUS (1e)	2.6.	2-8
Section 7.	GENERAL DESCRIPTION/PURPOSE (1f) ...	2.7.	2-9
Section 8.	SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS (1g)	2.8.	2-9
Section 9.	INFORMATION CONTACT(S) (1h)	2.9.	2-9

(This page intentionally left blank)

Chapter 2

GENERAL

2.1. GENERAL. This chapter describes the first component of the SSP. This component requires identification information about the computer system being reported. The title of each section of this chapter corresponds to a block in the SSP. For assistance, the corresponding SSP block numbers have been provided following each section title. Figure 2-01 contains examples of completed Basic System Identification components. Refer to these examples while going through this chapter. Only one computer system (or cluster) can be reported in the SSP.

2.2. RESPONSIBLE ORGANIZATION (1a). The responsible organization is the specific Marine Corps entity that has authority over of the Major Application(AIS) or the General Support System being reported. Another way to describe the responsible organization is in terms of ownership of the data and/or hardware. It is not unusual for this responsibility to change because of the LCM process, AIS implementation, organizational structure or the relocation of hardware/software. It is essential that the SSP be kept up to date and reviewed at least annually. If a contractor is involved, a Marine Corps organization must also be listed and the relationship described in the block for System Environment and Special Considerations, (1g) section of the SSP.

2.2.1. Major Application(AIS). The Functional Manager for Class I AISs would be a HQMC staff agency. For other than Class I AISs, the Functional Manager would be the designated organization within the Fleet Marine Force (FMF) or Supporting Establishment (SE). Figure 2-02 provides examples of responsible organizations for both Major Applications(AIS) and GSS.

2.2.2. General Support System (GSS). For GSS, the responsible organization should assign an individual to prepare an SSP with knowledge of the GSS being reported. This individual does not have to be in a security billet or a data processor in order to complete the SSP.

2.3. SYSTEM NAME/TITLE (1b). Logical boundaries must be drawn around the various processing, communications, storage, and related resources in order to define a system. For planning purposes, those systems under the same direct management control with essentially the same function, characteristics, and security needs may be treated as a single system. Every system name/title must be both meaningful and distinct from other system names/titles.

1. BASIC SYSTEM IDENTIFICATION - Major Application(AIS) Page 1 of 3

a. Responsible Organization.

MANPOWER MI

(Functional Manager)

b. System Name/Title: JUMPS/MMS

c. System Category
[X] AIS
[X] Class I
[ ] Class II
[ ] Class III

d. Processing Location:
MCCDPAs

Data Input Location:
Unit Diary - Marine Corps-wide

e. System Operational Status:
[X] Operational
[ ] Under Development

[ ] Locations are identified on on Continuation of Basic System Identification (Page ___)

f. General Description/Purpose: JUMPS/MMS is an integrated system of automated pay and manpower information reporting procedures, centralized processing, and distributed data bases. The system provides for recording, processing, and maintaining of military personnel and pay data on a continuing basis. It provides information for pay, personnel administration, and manpower management.

g. System Environment and Special Considerations: System interfaces with ARMS, MMAS, OPRAMS, DEERS, PREPASRPPA, SYSS, AND AFRS. This system is mission critical, deployable, transactiondriven, batch oriented, and updated twice a month. This AIS is a mainframe application running under the IBM operating system, MVS/XA.

h. Information Contacts:

NAME	TITLE	ORGANIZATION ADDRESS	PHONE: AV	PHONE: COMM
COL I.M. Cistem	Head, MI	HQMC (Code MI), Washington D.C. 20380	278-9600	614-9600

FIGURE 2-01
Completed Basic System Identification (AIS)

1. BASIC SYSTEM IDENTIFICATION - General Support System (GSS) Page 1 of 4

a. Responsible Organization:
HQMC, C4I2 Dept. C4 Div (CCIS)

b. System Name/Title: CCIS Office

c. System Category:

☐ LAN

☒ Cluster of Small Computers

☐ Stand Alone Small Computer

d. ☐ Make/Model/Serial #/Location:

☒ Location and information is listed on Continuation of Basic System Identification (Page 4)

☐ HW/SW Inventory Attached

e. System Operational Status:

☒ Operational ☐ Under Development

f. General Description/Purpose: The CCIS office microcomputers are used to support general administrative and IRM functions. Software includes Wordperfect 5.0, Multimate, DBase III Plus, Enable, and Harvard Graphics. There is no classified processing and all of the microcomputers are part of HQMC LAN.

g. System Environment and Special Considerations: There are no special considerations or unique systemenvironments that would cause special security concerns. The applications executed on these microcomputers are run under the basic DOS environment while the LAN access is via 3-COM EtherNET LAN operating system.

h. Information Contacts:

NAME	TITLE	ORGANIZATION ADDRESS	PHONE: AV	PHONE: COMM
LtCol M.M. Smith	Head, CCIS	HQMC, C4I2 Dept. C4 Div. (CCIS) Wash D.C. 20380	224-1111	(703) 614-1111
Mr. I.M. Saphe	Computer Security	HQMC, C4I2 Dept. C4 Div. (CCIS) Wash D.C. 20380	224-1111	(703) 614-1111

FIGURE 2-01 (cont.)
Completed Basis System Identification (GSS)

CONTINUATION OF BASIC SYSTEM IDENTIFICATION — MAJOR APPLICATIONS (AIS) Page ___ OF ___

MAKE	MODEL	LOCATION	STATUS

FIGURE 2-01 (cont.)
Continuation of Basic System Identification (AIS)

CONTINUATION OF BASIC SYSTEM IDENTIFICATION – GENERAL SUPPORT SYSTEM (GSS)
Page 4 OF 4

MAKE	MODEL	SERIAL NUMBER	LOCATION	STATUS
IBM PS2	Mod 60Z	72-7064124	HQMC, CCIS, RM 3018	Unassigned
Memorex-Telex	Mod 7086D	190000304	HQMC, CCIS, Rm 3018	LtCol Smith
IBM PS2	Mod 60Z	72-7062980	HQMC, CCIS, Rm 3018	Unassigned
IBM PS2	Mod 60Z	72-7064192	HQMC, CCIS, Rm 3018	Unassigned
Zenith Z-248	Adv System	649AC1333	HQMC, CCIS, Rm. 3020	Mr. Green
IBM PS2	Mod 60Z	72-7067663	HQMC, CCIS, Rm. 3020	Ms. White
COMPAQ DESKPRO	Mod 40	4725AJ2B0399	HQMC, CCIS, Rm. 3023	Capt Jones
IBM PS2	Mod 60Z	72-7062876	HQMC, CCIS, Rm. 3023	Maj House
Zenith Z-248	Adv System	811AE1020	HQMC, CCIS, Rm. 3023	Capt Johnson
Zenith Z-248	Adv System	649AC0884	HQMC, CCIS, Rm. 3023	Unassigned
Epson	Equity II+	0252054434	HQMC, CCIS, Rm. 3023	Capt Martin
Zenith Z-248	ZWX-248-62	649AC1314	HQMC, CCIS, Rm. 3023	Unassigned
Zenith Z-248	Adv System	814AE0467	HQMC, CCIS, Rm. 3023	Maj Williams
Zenith Z-248	Adv System	649AC1273	HQMC, CCIS, Rm. 3023	Mr. Wilson
Zenith Z-248	ZWX-024862	814AE0183	HQMC, CCIS, Rm. 3023	Unassigned
IBM PS/2	Mod 60Z	72-7064192	HQMC, CCIS, Rm. 3023	Ms Stevens
Epson	Equity II+	252054538	HQMC, CCIS, Rm. 3023	1LT Lacey
Zenith Z-248	Adv System	814AE0572	HQMC, CCIS, Rm. 3023	Maj Monday
Zenith Z-248	Adv System	649AC1315	HQMC, CCIS, Rm. 3023	Unassigned

FIGURE 2-01 (cont.)
Continuation of Basic System Identification (GSS)

AIS	Functional Manager
SABRS	HQMC Fiscal
PMC System	CG MCB CLNC
GSS	**Responsible Organization**
HQMC LAN	HQMC, AR
C4 Recall Roster	HQMC, C4
Personnel Information System	CO, Recruiting Station

FIGURE 2-02
Responsible Organization

Figure 2-03 contain examples of system names and titles.

JUMPS/MMS (AIS)
M3S (Developing AIS)
HQMC LAN (GSS)
Quantico Disbo Office (GSS)

FIGURE 2-03
System Name/Title

2.4. SYSTEM CATEGORY (1c). Each Sensitive Unclassified system must be identified. Major Application(AIS) can be Class I, II, or III. GSS can be identified as a LAN, a cluster of small computers (25 or less) or a stand-alone small computer.

2.5. LOCATION INFORMATION (1d). Update the SSP whenever a significant change occurs. The SSP does not need to be modified for temporary situations, (i.e. deployment).

2.5.1. Major Applications(AIS). For Major Applications(AIS), the functional manager must identify both the processing sites (i.e. MCCDPA, RASC, OR RJE) and the data input locations (i.e. local functional users-Marine Corps-wide) unless the hardware is a part of the exported AIS. Then, Identify those exported locations. Use the Continuation of Basic Identification (AIS) if additional space is needed. Figure 2-01 (cont.) on page 2-6 is an example of the Continuation of Basic System Identification (AIS).

2.5.2. GSS. For a GSS, identify the make, model and location of the system(s). Use the Continuation of Basic System Identification (GSS), Figure 2-01 (cont.) on page 2-7, when additional space is needed. If there is an accountability system already in place that reflects the requested hardware and software information, check the appropriate box, and if possible, attach a copy of the inventory to the SSP.

2.6. SYSTEM OPERATIONAL STATUS (1e). The operational status must be included for each system from one of the following:

- **Operational** - System is currently in operation.

- **Under Development** - System is currently under design, development, or implementation. For Major Applications(AIS), include the appropriate LCM phase of development and annotate the methods being used to assure that up-front security requirements are being included. Indicate the anticipated completion date.

2.7. GENERAL DESCRIPTION/PURPOSE (1f). Identify the function and purpose of the system. This should be a brief narrative, that provides a clear picture about the system. Extracts from the Mid-Range Information Systems Plan (MRISP) are good examples of general descriptions and purpose. Include all computer security requirements that are coordinated between end users and those responsible for any support system(s) being used. If describing a GSS, indicate the main features of the GSS and the applications being supported. Figure 2-04 contains an example of a General Description/Purpose for a Major Application(AIS) and a GSS.

Major Application(AIS): Class I ALPS files are used for various retrievals including sick leave earned and used, fringe benefits report, labor and time cards, personnel alpha listings, work center totals report, and fund code totals report.
General Support System: A system that is used to support daily administration and business functions through wordprocessing, database and spreadsheet utilities. The main features include Personnel data, budget and contracting information.

FIGURE 2-04
General Description/Purpose

2.8. SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS (1g). The System Environment and Special Considerations is a brief general description, that identifies any environmental factors that cause special security concerns or conditions that are unique or critical to this system. Figure 2-05 contains an example of a system environment and special considerations.

2.9. INFORMATION CONTACT(S) (1h). Information contact(s) include the name, title, organization address, and telephone numbers of one or more persons designated to be the point of contact for this system. The designated person(s) should have sufficient knowledge of the system to be able to provide additional information or points of contact as needed. It is important that the SSP be updated whenever this information is

changed or modified. Figure 2-06 contain examples of information contacts.

- System is located in harsh or overseas environment; Software is rapidly implemented; system is an open network used by the general public or with overseas access; System is processed at a facility outside of the Marine Corps' control;
- There are no system environment or special considerations unique or critical to this system.

FIGURE 2-05
System Environment and Special Considerations

NAME	TITLE	ORGANIZATION ADDRESS	AV	COMM
MAJ Smith	Func Mgr	HQMC Manpower (MI)	224-0000	(703)614-0000
Mr. Jones	Budg An	HQMC Fiscal (FDB)	224-0001	(703)614-0001

FIGURE 2-06
Information Contact(s)

Chapter Table of Contents

Chapter 3

SENSITIVITY OF INFORMATION HANDLED

	Paragraph	Page
Section 1. GENERAL	3.1.	3-3
Section 2. MID-RANGE INFORMATION SYSTEMS PLAN (MRISP)	3.2.	3-3
Section 3. GENERAL DESCRIPTION OF INFORMATION SENSITIVITY (2a)	3.3.	3-3
Privacy Data	3.3.1.	3-3
National Interest Data	3.3.2.	3-3
Section 4. SYSTEM CLASSIFICATION (2b)	3.4.	3-7
Section 5. APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM (2c)	3.5.	3-7
Section 6. PROTECTION REQUIREMENT (2d)	3.6.	3-7
Confidentiality (2d.1)	3.6.1.	3-7
Integrity (2d.2)	3.6.2.	3-8
Availability (2d.3)	3.6.3.	3-8
Section 7. LEVEL OF PROTECTION (2e)	3.7.	3-8

(This page intentionally left blank)

Chapter 3

SENSITIVITY OF INFORMATION HANDLED

3.1. GENERAL. This section of the SSP addresses the sensitivity of information and provides a description of the types of information handled by the system which then in-turn establishes the basis for the system's security requirements. Figure 3-01 contains an example of a completed Sensitivity of Information Handled component from the SSP. Refer to this example while going through this chapter.

3.2. MID-RANGE INFORMATION SYSTEMS PLAN (MRISP). The Marine Corps requires all Major Applications(AIS) to follow the requirements of MCO P5231.1, Life Cycle Management for Automated Information Systems (LCM-AIS) Projects. The MRISP is a strategic AIS plan which describes the information resource needs of the Marine Corps and reflects the strategic planning effort in an annually updated plan. The reporting process by which all Marine Corps AISs are identified is through the MRISP. The MRISP collects, stores and publishes this information for each AIS. In support of the MRISP, information values requested in the SSP must be consistent with that which was reported in the MRISP. (At this time, GSS are not reported in the MRISP.)

3.3. GENERAL DESCRIPTION OF INFORMATION SENSITIVITY (2a). Sensitive Unclassified information can either be Privacy Data or National Interest Data.

3.3.1. Privacy Data. Privacy Data is Sensitive Unclassified information that is personal in nature and is protected specifically under the Privacy Act of 1974. The Privacy Act 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, regardless of whether the information system is maintained in personnel offices or in a separate information system used by the supervisor. Select the Privacy Data Code that best describes the data from the list of available codes contained in Figure 3-02.

3.3.2. National Interest Data. National Interest Data includes all other types of Sensitive information not included in the Privacy Data category. Select the National Interest Data Code that best describes the data from the list contained in Figure 3-03.

3.4. SYSTEM CLASSIFICATION (2b). Indicate the classification of the system.

2. SENSITIVITY OF INFORMATION HANDLED - Major Application(AIS) Page 2 of 3

a. General Description of Information Sensitivity:
Information Category (MRISP Code):
Privacy 1 - 7 [P 1] or National 1 - 13 [N ___]

b. System Classification:
[X] Sensitive Unclassified
[ ] OTHER (_____)

c. Applicable Laws or Regulations Affecting the System:
Public Law 93-579, Privacy Act of 1967
Federal Manager's Financial Integrity Act of 1982

(d) Protection Requirement:	(e) Level of Protection
(1) CONFIDENTIALITY: P.L. 93-579 mandates that all information concerning personnel be protected.	[X] Primary (P) [ ] Secondary (S) [ ] Minimal (M) MRISP Code [C P]
(2) INTEGRITY: Without the required protection, financial data and personnel information would be in jeopardy thus the reliability and accuracy of the information. This would be costly to all military personnel pay and allowances, privacy of information and jeopardize the system to potential fraud, waste, and abuse.	[X] Primary (P) [ ] Secondary (S) [ ] Minimal (M) MRISP Code [I P]
(3) AVAILABILITY:	[ ] Primary (P) [ ] Secondary (S) [ ] Minimal (M) MRISP Code [A ___]

FIGURE 3-01
Completed Sensitivity of Information Handled (AIS)

2. SENSITIVITY OF INFORMATION HANDLED - General Support System (GSS) Page 2 of 4

a. General Description of Information Sensitivity:
Privacy 1 - 7 or P ___
National 1 - 13 or N 13 ___
Not Applicable or NA ___

b. System Classification:
[X] Sensitive Unclassified
[ ] OTHER (_____)

c. Applicable Laws or Regulations Affecting the System:
OMB Circular A-130, Management of Information Resources

(d) Protection Requirement:	(e) Level of Protection
(1) CONFIDENTIALITY:	[ ] Primary (P) [ ] Secondary (S) [ ] Minimal (M) C ___
(2) INTEGRITY: Without protection requirements this information would be costly to replace in dollars, manpower, and time. In many instances, the information cannot be recreated.	[X] Primary (P) [ ] Secondary (S) [ ] Minimal (M) I P ___
(3) AVAILABILITY: Without protection requirements in place the ability to meet the demands from the field in a timely manner is jeopardized.	[ ] Primary (P) [X] Secondary (S) [ ] Minimal (M) A S ___

FIGURE 3-01 (cont.)
Completed Sensitivity of Information Handled (GSS)

P1	Individual Education, financial, medical history, criminal or investigation related, employment and personnel records including but not limited to fitness and evaluation reports, etc.
P2	Senior military officer assignment and promotion nominations (Military Manpower and Personnel Policy)
P3	Military promotion lists
P4	Child/Spouse abuse incident reports
P5	Civilian Personnel Policy, Congressional and White House inquiries
P6	Individual records which contain a name, identifying number, symbol, or identifying particular such as a fingerprint, voice, photograph. etc.
P7	Other privacy information not previously listed in the "P" (Privacy) category. (Records from the Chaplain, Judge Advocate General (JAG), Safety records, Training Records, etc.)

FIGURE 3-02
Privacy Data Codes

N1	Research, development, acquisition sustainment and force status data, War Reserve material data
N2	Information related to total force status data
N3	Commercial proprietary information, logistics records, maintenance records
N4	Information, industrial personnel, and operations security
N5	Travel itineries of high ranking-personnel
N6	Financial data
N7	Information regarding technologies identified in the Military Critical Technologies List (MCTL) and related research, development, test and evaluation activities.
N8	Information regarding research, development, test, and evaluation of technologies that would require a license for export
N9	Access control information (password, logon data, etc.)
N10	Congressional and White House inquiries
N11	Requirements for weapons systems
N12	Procurement actions, source selection sensitive data
N13	Other national interest information not previously listed in the "N" (National Interest) category, (automated decision-making aids (models), auditor reports, essential elements of friendly information (EEFI), etc.)

FIGURE 3-03
National Interest Data Codes

3.5. APPLICABLE LAWS OR REGULATIONS AFFECTING THE SYSTEM (2c). List any laws or regulations that establish specific requirements for confidentiality, integrity, and availability of information in the system. Examples might include the Privacy Act of 1974, Federal Manager's Financial Integrity Act of 1982, or a regulation that specifies how the information must be processed. Applicable laws or regulations should NOT be a list of technical standards concerning how to protect the system once the need for such protection has been determined, (i.e. FIPS PUB 73, Guidelines for Security of Computer Applications, etc.). However, these guidance and reference documents will be listed in the System Security Measures component of the SSP. In this regard, Appendix D is a comprehensive list of guidelines and documents on computer security that provide detailed information for implementing the public laws and directives contained in Appendix B. Note: If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act System(s) of records and whether the system(s) is used for computer matching activities.

3.6. PROTECTION REQUIREMENT (2d). Indicate the type and relative importance of protection needed for the identified system. Include an **impact statement** of the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or the modification of the information within the system. If possible, describe this impact in terms of specific values such as: **cost, the inability to carry out mandated functions, timeliness**, etc. A system can have up to two protection requirements, however, the MRISP can only accommodate one entry for an AIS. Use the "best fit" approach. The following are the three areas from which to base your protection requirements:

3.6.1. Confidentiality (2d.1). This term is not to be confused with the classification of the system. Confidentiality refers to the system containing information that requires protection from unauthorized disclosure. The information can be Sensitive Unclassified however its disclosure could compromise or become detrimental to the overall mission. Figure 3-04 contains examples of the types of information that would require protection for confidentiality reasons.

Timed Dissemination:	(Data used in a production cycle)
Personal Data:	(Covered under the Privacy Act)
Proprietary Information:	(Plans/decisions that affect an organization)

FIGURE 3-04
Information Requiring Confidentiality

3.6.2. Integrity (2d.2). Integrity refers to the system containing information which must be protected from unauthorized, unanticipated or unintentional modification. Integrity includes the detection of such activities as well. Without effective controls, the information becomes vulnerable to fraud, waste and abuse and acts of sabotage, thus jeopardizing the system's reliability. Figure 3-05 contains examples of the types of information that would require protection for integrity reasons.

JUMPS/MMS
Personnel Data Base
Supply Inventory

FIGURE 3-05
Examples of Systems Requiring Integrity Protection

3.6.3. Availability (2d.3). Availability refers to the system that contains information or provides services which must be protected from denial. In other words, the information must be available at all times or when required in order to meet mission requirements. Without this type of control measure protection, many decisions would be made based on outdated information or cause decisions to be postponed until the information was available. This would be costly in such areas as time and manpower. Figure 3-06 contains examples of the types of information that would require protection for availability reasons.

Air Traffic Control System
Economic Indicator Information
DEERS/Medical Data and Information

FIGURE 3-06
Examples of Systems Requiring Availability Protection

3.7. LEVEL OF PROTECTION (2e). A level of protection must be identified for each protection requirement category that has been identified in the previous section. There are three levels of protection: **Primary**, **Secondary**, or **Minimal**. A primary level indicates that there is a critical concern for the system under this category. A secondary level indicates that there is an important concern, but not necessarily paramount in the organization's priorities. A minimal level indicates that no protection is required. A minimal level protection requirement should be an unusual circumstance and will require a brief explanation as to why the information should not be protected or is of no importance. A high protection requirement can be used for more than one of the categories (confidentiality, integrity, availability) if necessary or appropriate. A letter is already provided in the block next to the categories on the SSP. Add a

"P", "S", or "M" to the first letter of the level of protection. Figure 3-07 contains examples of the information necessary for this entry.

Protection Requirement		Level of Protection		=	Code
Confidentiality (C)	+	Primary	(P)	=	CP
Integrity (I)	+	Primary	(P)	=	IP
Availability (A)	+	Secondary	(S)	=	AS
Availability (A)	+	Minimal	(S)	=	AM

FIGURE 3-07
MRISP Entry for Protection Requirement

(This page intentionally left blank)

Chapter Table of Contents

Chapter 4

SYSTEM SECURITY MEASURES

	Paragraph	Page
Section 1. GENERAL	4.1.	4-3
Section 2. RISK MANAGEMENT	4.2.	4-3
Methodology (3a)	4.2.1.	4-3
Section 3. SECURITY CONTROL MEASURES - MAJOR APPLICATIONS(AIS) (3c)	4.3.	4-7
Management Controls (3c.1)	4.3.1.	4-7
Development/Implementation Controls (3c.2) ..	4.3.2.	4-7
Operational Controls (3c.3)	4.3.3.	4-8
Security Awareness and Training Measures (3c.4)	4.3.4.	4-10
Technical Controls (3c.5)	4.3.5.	4-10
Complimentary Controls Provided by Support Systems (3c.6)	4.3.6.	4-12
Section 4. SECURITY CONTROL MEASURES - GENERAL SUPPORT SYSTEMS (GSS) (3c)	4.4.	4-12
Management Controls (3c.1)	4.4.1.	4-12
Acquisition/Development/Installation Controls (3c.2).....	4.4.2.	4-13
Operational Controls (3c.3)	4.4.3.	4-13
Security Awareness and Training Measures (3c.4)	4.4.4.	4-14
Technical Controls (3c.5)	4.4.5.	4-15
Controls Over the Security of Applications (3c.6)	4.4.6.	4-16
Section 5. GUIDANCE AND REFERENCES (3d)	4.5.	4-16
Section 6. SUPPORTING DOCUMENTATION (3e)	4.6.	4-16
Section 7. SECURITY CONTROL MEASURE STATUS (3e)	4.7.	4-16
Section 8. ADDITIONAL COMMENTS (4)	4.7.	4-17

(This page intentionally left blank)

Chapter 4

SYSTEM SECURITY MEASURES

4.1. GENERAL. This component of the SSP describes the control measures, in place or planned, that are intended to meet and support the protection requirements of the system. The types of control measures should be consistent with the need for the protection of the system described in the previous chapters. This section is very important and can be of help when a risk analysis and a system accreditation, initial or update, must be conducted. In order to determine what security measures are needed in providing the required protection for the Sensitive Unclassified information on the system, a risk analysis must be conducted. The Security Control Measures identified in Section 4 of this Chapter are the minimal control measures that must be addressed for every system. Figure 4-01 contains completed examples of System Security Measures for a Major Applications(AIS) and a GSS. Each control measure must have corresponding references, guidelines, and status supporting the protection requirements identified.

4.2. RISK MANAGEMENT. Risk management is a crucial element of the security planning process. The risk management process identifies:

- informational and other assets of the system,

- threats that could affect the confidentiality, integrity, and availability of the system,

- important system vulnerabilities to the threats,

- potential impacts from threat activity,

- protection requirements to control the risks, and

- appropriate security measures.

4.2.1. Methodology

a. Formally Documented Risk Analysis (3a). A formal risk analysis consists of a structured approach to identify assets, determine threats and vulnerabilities, estimate potential impacts, identify applicable controls and their costs, and select cost-effective controls for use.

b. Name/Description (3b). If a formally documented risk analysis is used, include the name of the methodology used and any associated automated tools. Briefly describe the methodology or approach used, such as an in-house developed approach to risk analysis.

3. SYSTEM SECURITY MEASURES - MAJOR APPLICATIONS(AIS) Page 3 of 3

a. Risk Analysis Method: ☐ Formal ☒ Other | b. Name: In-House Method (Qualitative)

c. Security Control Measures:	d. Guidance and References	e. Supporting Documentation	f. Status SCM Code	Date
(1) Management Controls:				
(A) Assignment of Security Responsibilities	IRM 5239-07,08	NAC/NACI/DNACI	(a) I	1989
		ENTNAC	(b) I	1989
(B) Personnel Screening		SF 171		
(2) Development/Implementation Controls				
(A) Security Specifications	IRM 5239-08	Test Plans	(a) I	1989
(B) Design Review and Testing	IRM 5231-01,06,14,17	Security Checklists	(b) I	1989
(C) Certification	MCO P5231.1	Risk Assessments	(c) I	1989
(D) ST&E		Completed ST&Es	(d) I	1989
(E) Risk Assessment		Certification Documents	(e) I	1989
		Accreditation Documentation		
(3) Operational Controls:	IRM 5239-08,10,12	Security Checklists	(a) I	1989
(A) Physical and Environment Protection	IRM 5231-10,14,17,19	Control Log Books	(b) I	1989
(B) Production I/O Controls	IRM 5234-01,03	Contingency Plan	(c) I	1989
(C) Emergency, Back-up, Contingency Planning		Maintenance Contracts	(d) I	1989
(D) Audit and Variance Detection		System Audit	(e) I	1989
(E) Documentation		Documentation	(f) I	1989
(F) Application SW Maintenance Controls		Local SOP	(g) I	1989
(G) HW/System SW Maintenance Controls		MENS		
(4) Security Awareness/Training Measures:	IRM 5239-08,10,12	Training Plan	(a) I	1989
(A) Program/Activities	Computer Security Act 1987	Individual Training Records		
(5) TECHNICAL CONTROLS:	IRM 5239-08,07,08,10,12	TSO Documentation	(a) I	1989
(A) User Identification/Authentification		Local MFRs	(b) I	1989
(B) Authorization/Access Controls		SOP	(c) I	1989
(C) Data Integrity/Validity Controls			(d) I	1989
(D) Audit Trails and Journaling				

FIGURE 4-01
Completed System Security Measures (AIS)

3. SYSTEM SECURITY MEASURES - MAJOR APPLICATION(AIS) (Cont.) Page ___of___				
c. Security Control Measures:	d. Guidance and References	e. Supporting Documentation	f. Status SCM Code	Date
(6) Complementary Controls Provided by support Systems				
4. ADDITIONAL COMMENTS				

FIGURE 4-01 (cont.)
Continued System Security Measures (AIS)

3. SYSTEM SECURITY MEASURES - GENERAL SUPPORT SYSTEM (GSS) Page 3 of 4

a. Risk Analysis Method: ☐ Formal ☒ Other (b). Name: In-House (Qualitative)

c. Security Control Measures:	d. Guidance and References	e. Supporting Documentation	f. Status SCM Code		Date
(1) Management Controls:					
(A) Assignment of Security Responsibilities	IRM 5239-07,08	NAC/NACi/DRACI	(A)	1	6/90
(B) Personnel Screening		SF 171	(B)	1	1990
(C) Risk Analysis		ENTNAC	(C)	P	1991
(2) Acquisition/Development/Installation Ctls					
(A) Acquisition Specifications	IRM 5239-08	SOP	(A)	N/A	
(B) Accreditation	IRM 5231-06,14,17	MFR'S	(B)	P	1991
(C) Certification		Accreditation/Certification Documents	(C)	P	1991
(3) Operational Controls:					
(A) Physical and Environment Protection	IRM 5239-08,10,12 IRM 5231-10,14,17,19 IRM 5234-01,03	SOP	(A)	1	1990
(B) Production, I/O Controls		Security Checklists	(B)	N/A	
(C) Emergency, Back-up, Contingency Planning			(C)	P	1991
(D) Audit and Variance Detection			(D)	N/A	
(E) HW and System SW Maintenance Controls			(E)	P	1991
(F) Documentation			(F)	I/P	80/91
(4) Security Awareness/Training Measures:	IRM 5239-08,10,12 Computer Security Act 1987	Security Awareness and Training Ltrs Personnel Sign-In	(A)	IP	89/91
(A) Security Awareness and Training Measures					
(5) TECHNICAL CONTROLS:	IRM 5239-06,07,08,10,12	System SW Controls	(A)	I	1986
(A) User Identification/Authentification			(B)	N/A	
(B) Authorization/Access Controls			(C)	N/A	
(C) Integrity Controls			(D)	N/A	
(D) Audit Trails Mechanisms			(E)	N/A	
(E) Confidentiality Controls					
(6) Controls Over The Security of Applications:				N/A	

FIGURE 4-01 (cont.)
Completed System Security Measures (GSS)

4.3. SECURITY CONTROL MEASURES - MAJOR APPLICATIONS (AIS) (3c). Ensure that you use the correct control measures for the computer system. Many of the security control measures are the same for both Major Applications(AIS) and GSS. However, some control measures are unique to each type of system. The following paragraphs give the overall requirements for security control measures necessary for each system. The controls should be addressed from the perspective of the responsible organization having direct management responsibility for the system. The controls are derived from requirements and guidance in the Computer Security Act, OMB Circular A-130 (Appendix III)," Management of Federal Information Resources," and publications produced by the National Institute of Standards and Technology. There may be additional security control measures that are unique to your command. Add these to the appropriate control measure section or create another subheading to fit the new control measure. The following are the security control measures required for Major Applications(AISs).

4.3.1. Management Controls (3c.1). These pertain to the overall management controls of the application system.

a. Assignment of Security Responsibility (3c.1.A). An individual will be appointed as the responsible individual for the security measures pertaining to the application system. IRM-5239-06, Data Access Security, IRM-5239-07, Terminal Area Security Officer (TASO) and IRM-5239-08, Computer Security Procedures will provide guidance in appointing security personnel.

b. Personnel Screening (3c.1.B). Personnel security policies and procedures should be in place. The objective is to authorize access and processing privileges to individuals on an as needed basis only within the application system. Such requirements include screening individuals with access to the application as well as those participating in the design, development, operation, or maintenance of the application. IRM-5239-08, Computer Security Procedures clearly defines personnel selection and screening requirements.

4.3.2. Development/Implementation Controls (3c.2). Procedures to assure that protection is built into the system, especially during system development. IRM-5231-01 System Development Methodology provides the requirements for security throughout the life cycle of an AIS.

a. Security Specifications (3c.2.A). Appropriate technical, administrative, physical, and personnel security requirements should be specified for the application. IRM-5239-08, Computer Security Procedures provides guidance on security specifications.

b. Design Review and Testing (3c.2.B). A design review and systems test is usually performed for an application prior to placing it into operation to assure the application meets the security specifications. The results of the design reviews and

system tests should be fully documented and maintained by the Project Manager or responsible organization. References include IRM-5231-06, Detailed Design Specification and IRM-5231-14, Test Plan.

c. Certification (3c.2.C). The Designated Approving Authority (DAA) must have certified that the application meets all applicable Federal policies, regulations, and standards, and that safeguards appear adequate **prior** to the application being placed into operation. If the application has been in operation for a period of time, it should have been audited or reviewed and recertified within the last three years. Indicate the applicable dates. IRM-5231-17, Inspection and Acceptance and IRM-5239-08, Computer Security Procedures provide guidance for Certification.

d. Security Test and Evaluation (ST&E) (3c.2.D). The Security Test and Evaluation (ST&E) is a process to determine whether the system administrative, technical, and physical security measures are functioning adequately. It requires documenting and reporting the test findings to the appropriate authorities and to make recommendations based on the test results. IRM-5239-11, Accreditation Process, provides guidance in this area.

e. Risk Assessment (3c.2.E). Risk assessment is a means of identifying threats that would have a negative impact on the mission of an organization. The risk assessment process provides the following benefits:

- Quantitative or qualitative guidance in order to determine the amount of resources reasonable to expend on security measures.

- Guidance for long range planning for site selections, building designs, hardware configurations, procurements, software systems, and internal controls.

- Criteria for designing and evaluating contingency plans.

- Security policies at the organization level that further identify threats, the resources to protect, and local security responsibilities.

- Assessment of damage caused by an unfavorable event and predicting the frequency of that unfavorable event.

Risk assessment includes the areas of personnel, physical environment, hardware and software systems, data communications, AIS applications, and operations. IRM-5239-11, Accreditation Process, provides guidelines for this area.

4.3.3. Operational Controls (3c.3). It is essential that day-to-day procedures and mechanisms are not only protected but

documented. These controls include the requirements of Functional Managers and end users.

a. Physical and Environmental Protection (3c.3.A). Adequate physical protection of the area where system application processing takes place as well as day-to-day operational procedures is necessary. In the event that the present control measures are not adequate, indicate the plans for installing security measures and identify when they will become operational. Examples of these include locks on the terminals, physical barriers around the processing area, alarms on doors and windows, and counters within the area restricting authorized personnel traffic around processing. IRM-5139-08, Computer Security Procedures, IRM-5239-10, Small Computer Systems Security, and IRM-5239-12, Project Manager's Security Handbook all provide sound guidance for physical and environmental protection.

b. Production and I/O Controls (3c.3.B). Production and I/O controls include the proper handling, processing, storage, and disposal of input and output data and media, as well as access controls on the data and media itself. This includes media labels and the distribution processes. IRM-5231-08, Computer Operations Manual, IRM-5239-08, Computer Security Procedures, and IRM-5239-10, Small Computer Systems Security provide guidance on production and I/O controls.

c. Emergency, Backup, and Contingency Planning (3c.3.C). It is important that workable procedures be in place to ensure unvarying performance of essential functions continue in the event that information technology support is interrupted. These contingency alternatives should be coordinated with the back-up and recovery plans of any installation and/or network used by the application. IRM-5239-08, Computer Security Procedures, IRM-5239-09, Contingency Planning, IRM-5239-10, Small Computer Systems Security, and IRM-5239-12, Project Manager's Security Handbook provide guidance for emergency, backup, and contingency measures.

d. Audit and Variance Detection (3c.3.D). Audit and variance detection controls allow management to conduct an independent review of records and activities to test the adequacy of such controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection for an application checks for anomalies in such things as the numbers and types of transactions, volume and dollar thresholds, and other deviations from standard activity profiles. IRM-5231-10, Quality Assurance Plan; IRM-5231-14, Test Plan; IRM-5231-17, Inspection and Acceptance; IRM-5239-08, Computer Security Procedures; IRM-5239-10, Small Computer Systems Security, and IRM-5239-12, Project Manager's Security Handbook all provide guidance and procedures for effective audit and variance detection.

e. Application Software Maintenance Controls (3c.3.E). Application software and maintenance controls are used to monitor

the installation of and updates to application software. The purpose is to ensure that the software functions as expected and that an historical record is maintained of all application system changes. Such controls also help to ensure that only authorized software is allowed on the system. These controls may include a software configuration policy that grants managerial approval to modifications and then documents the changes. They also should include products used for virus protection. IRM-5234-01, Programming Standards and IRM-5234-03, Systems Software provides guidance on application software maintenance controls.

f. Documentation (3c.3.F). There should be controls in the form of descriptions of the hardware, software, policies, standards, and procedures related to computer security, to include backup and contingency activities. Also included are descriptions of end user procedures. Documentation should be coordinated with the computer facility and/or network manager(s) to ensure that adequate application and installation documentation is maintained and available to provide continuity of operations. IRM-5231-01, System Development Methodology (SDM) Overview provides the guidelines for required documentation for AISs.

g. Hardware and System Software Maintenance Controls (3c.3.G). Hardware and system software maintenance controls are used to monitor the installation of hardware, operating system updates and other system software to ensure that they function as expected and that an historical record is maintained of these changes. These controls may also be used to ensure that only authorized software is allowed on the system. Controls of this type may include hardware and system software configuration policy that grants managerial approval to modifications, as well as document the changes. They may also include products useful for "virus" protection. IRM-5231-09A, Application Configuration Management Plan, MCO P5231.1B, LCM-AIS Projects and local Standing Operating Procedures (SOPs) provide guidelines for these security controls.

4.3.4. Security Awareness and Training Measures (3c.4)

a. Program Activities (3c.4.A). All employees involved with the management, use, or operation of the application should be aware of their security responsibilities and trained adequately on how to fulfill them. IRM-5239-08, Computer Security Procedures; IRM-5239-10, Small Computer Systems Security, IRM-5239-12, Project Manager's Security Handbook, and the Computer Security Act 1987 all provide guidance on security awareness and training requirements.

4.3.5. Technical Controls (3c.5). Technical controls include hardware and software measures used to provide automated and/or manual protection. Normally these types of controls are coordinated with the network and/or computer facility manager. IRM-5239-09, Contingency Planning provides the guidance for this type of security control.

a. User Identification and Authentication (3c.5.A). User identification and authentication controls are used to provide automated and/or manual protection. Normally these types of controls are coordinated with the network and/or data center manager. They identify or verify the eligibility of a Marine Corps entity, originator, or individual to access specific categories of information, to perform an activity, or to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification. Such controls include the use of passwords, tokens, biometrics or other personal mechanisms to authenticate identity. IRM-5239-06, Data Access Security; IRM-5239-07, Terminal Area Security Officer (TASO); IRM-5239-08, Computer Security Procedures; IRM-5230-10, Small Computer Security Procedures; and IRM-5239-12, Project Manager's Security Handbook are references that provide guidance in this area.

b. Authorization/Access Controls (3c.5.B). Authorization and Access controls are hardware or software features that are designed to permit only authorized access to the application and/or to detect or prevent unauthorized access. IRM-5239-06, Data Access Security; IRM-5239-07, Terminal Area Security Officer (TASO); IRM-5239-08, Computer Security Procedures; IRM-5239-10, Small Computer Systems Security; and IRM-5239-12, Project Manager's Security Handbook provides guidance.

c. Data Integrity/Validation Controls (3c.5.C). Data integrity/validation controls are used to protect data from accidental or malicious alteration or destruction, and provide assurance to the user that the data meets an expectation about its quality. These are usually hardware or software features that are designed to permit only authorized access to or within the application to restrict users to authorized transactions and functions, and/or to detect unauthorized activities. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements. Message authentication is an example of this category of control. IRM-5239-06, Data Access Security; IRM-5239-07, Terminal Area Security Officer (TASO); IRM-5239-08, Computer Security Procedures; IRM-5239-10, Small Computer Systems Security, and IRM-5239-12 Project Manager's Security Handbook provide guidance pertaining to these types on controls.

d. Audit Trails and Journaling (3c.5.D). Audit trails and journaling controls provide a transaction monitoring capability chronologically recording application activities. This enables the reconstruction of a transaction from its inception to final results including any modification of files along the way. IRM-5239-06, Data Access Security; IRM-5239-07, Terminal Area Security Officer (TASO); IRM-5239-08, Computer Security Procedures; IRM-5239-10, Small Computer Systems Security; and IRM-5239-12, Project Manager's Security Handbook are references that provide the necessary guidance for audit trails.

4.3.6. Complementary Controls Provided by Support Systems (3c.6). The person responsible for the Major Application(AIS) should understand and accept the risk inherent in processing on the network or at the installation(s) that supports the application. If not, plans for greater understanding of that risk should be described. Each Major Application(AIS) will have different environments and ultimately different risks. Therefore, careful consideration should be given in order to identify additional or potential areas for concern that are inherently unique to that AIS.

4.4. SECURITY CONTROL MEASURES - GENERAL SUPPORT SYSTEMS (GSS) (3c). Ensure that you use the correct control measures for the computer system. Many of the security control measures are the same for both Major Applications(AIS) and GSS. However, some measures are unique to each type of system. Controls included should be addressed from the perspective of the responsible organization having direct management responsibility for the system. The controls are derived from requirements and guidance in the Computer Security Act, OMB Circular A-130 (Appendix III)," Management of Federal Information Resources," and publications produced by the National Institute of Standards and Technology. There may be additional security control measures that are unique to your command. Add these to the appropriate control measure section or create another subheading to fit the new control measure.

4.4.1. Management Controls (3c.1). These are overall management security controls for a General Support System.

a. Assignment of Security Responsibilities (3c.1.A). An individual is to be appointed as the responsible individual for the security of each GSS. The individual should become knowledgeable in information technology and security matters. IRM-5239-06, Data Access Security and IRM-5239-08, Computer Security Procedures, provides guidance in appointing security personnel.

b. Personnel Screening (3c.1.B). Personnel security policies and procedures should be in place and working to control access to and within the GSS. Such requirements include the screening of individuals with access to the systems as well as those participating in any design, development, operation, or maintenance of local general applications. IRM-5239-08, Computer Security Procedures clearly defines personnel selection and screening requirements.

c. Risk Analysis (3c.1.C). A risk analysis consists of a structured approach to identify assets, determine threats and vulnerabilities, estimate potential impacts, identify applicable controls and their costs, and select cost effective controls for use. Include the name of any automated or formalized manual methodology used.

4.4.2. Acquisition/Development/Installation Controls (3c.2)

a. Acquisition Specifications (3c.2.A). Appropriate technical, administrative, physical, and personnel security requirements are to be included in specifications for the acquisition or operations of information technology installations, equipment, software, and related services. IRM-5239-08, Computer Security Procedures provides guidance on security specifications.

b. Accreditation/Certification (3c.2.B). Accreditation is management authorization and approval to process sensitive information in an operational environment. The accreditation is issued by a Designated Approval Authority (DAA) and usually includes any constraints for processing in the environment. It is normally based on a certification which is a technical evaluation that indicates how well a design/implementation meets a specified set of computer security requirements. Indicate the applicable dates of accreditation/certification or when the accreditation/certification is scheduled. IRM-5231-17, Inspection and Acceptance, IRM-5239-08, Computer Security Procedures, IRM-5239-10, Small computer Systems Security and IRM-5239-11, Accreditation Process provides guidance for Certification.

4.4.3. Operational Controls (3c.3). Operational controls are day-to-day procedures and mechanisms to protect operational systems. Normally these are found in the local SOP.

a. Physical and Environmental Protection (3c.3.A). Physical and environmental protection controls are used to protect against a wide variety of threats and hazards to include deliberate intrusions, natural or man-made hazards, and utility outages or breakdowns. Some examples of protection measures include locks on the terminals, physical barriers around offices containing hardware, alarms on doors and windows, special fire fighting equipment, "hardened" communications, and surge protectors on electrical equipment. IRM-5139-08, Computer Security Procedures, IRM-5239-10, Small Computer Systems Security, and IRM-5239-12, Project Manager's Security Handbook all provide sound guidance for physical and environmental protection.

b. Production and I/O Controls (3c.3.B). Production and I/O controls are the proper handling, processing, storage, and disposal of input and output data and media from the GSS as well as access controls to the data and media itself. This includes media labeling, the distribution processes, and disposal of input and output from the support system. IRM-5231-08, Computer Operations Manual, IRM-5239-08, Computer Security Procedures, and IRM-5239-10, Small Computer Systems Security provide guidance on production and I/O controls.

c. Emergency, Backup, and Contingency Planning (3c.3.C). Emergency, backup, and contingency planning provide workable procedures for the unvarying performance of essential functions

to continue in the event that information technology support is interrupted. Appropriate alternatives should be coordinated with the back-up and recovery plans of all the installations and/or networks used by the GSS. These plans should be made known to users and coordinated with their plans. IRM-5239-08, Computer Security Procedures, IRM-5239-09, Contingency Planning, IRM-5239-10, Small Computer Systems Security, and IRM-5239-12, Project Manager's Security Handbook provide guidance for emergency, backup and contingency measures.

d. Audit and Variance Detection (3c.3.D). Audit and variance detection are controls which allow management to conduct an independent review of systems' records and activities in order to test for adequacy of system controls. They also provide a means to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users. IRM-5231-10, Quality Assurance Plan, IRM-5231-14, Test Plan, IRM-5231-17, Inspection and Acceptance, IRM-5239-08, Computer Security Procedures, IRM-5239-10, Small Computer Systems Security, and IRM-5239-12, Project Manager's Security Handbook all give guidance and procedures for effective audit and variance detection.

e. Hardware and System Software Maintenance Controls (3c.3.E). Hardware and system software maintenance are controls used to monitor the installation of and updates to GSS software. The purpose is to ensure that the software functions as expected and that an historical record is maintained of all system changes. Such controls also help to ensure that only authorized software is allowed on the system. These controls may include software configuration policy that grants managerial approval to modifications and then documents the approved changes. These types of controls increase virus protection. Local SOPs should include guidance and procedures.

f. Documentation (3c.3.F). There should be controls in the form of descriptions of the hardware, software, policies, standards, and procedures related to computer security, to include backup and contingency activities. Also included are descriptions of end user procedures. Documentation should be coordinated with the computer facility and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations. Local SOPs should provide the guidance and procedures.

4.4.4. Security Awareness and Training Measures (3c.4). All employees involved with the management, use, or operation of the application should be aware of their security responsibilities and trained adequately on how to fulfill them. IRM-5239-08, Computer Security Procedures, IRM-5239-10, Small Computer Systems Security, IRM-5239-12, Project Manager's Security Handbook, and Computer Security Act 1987 all provide guidance on security awareness and training measures.

4.4.5. Technical Controls (3c.5). Technical controls are hardware and software security controls implemented to protect GSS from unauthorized access or misuses, to facilitate detection of security violations, and to support security requirements for associated applications.

a. User Identification and Authentication (3c.5.A). User identification and authentication controls are used to identify or verify the identity of a station, originator, or individual prior to allowing access to the system or specific categories of information within the system. Such controls may also be used to verify that those authorized personnel are only performing those tasks in accordance with their access privileges. Such controls include the use of passwords, tokens, biometrics or other personal mechanisms to authenticate identity. IRM-5239-06, Data Access Security, IRM-5239-07, Terminal Area Security Officer (TASO), IRM-5239-08, Computer Security Procedures, and IRM-5230-10, Small Computer Security Procedures provide the necessary guidelines.

b. Authorization/Access Controls (3c.5.B). Authorization and Access controls are hardware or software features, such as an access list, that are designed to permit only authorized access to the data and/or to detect or prevent unauthorized access. This includes controls to restrict access to the operating system, limits on access to programming resources, and controls to support security policies of associated applications. IRM-5239-06, Data Access Security, IRM-5239-07, Terminal Area Security Officer (TASO), IRM-5239-08, Computer Security Procedures, and IRM-5239-10, Small Computer Systems Security provide guidelines and procedures for authorization and access controls.

c. Integrity Controls (3c.5.C). Integrity controls are used to protect the operating system, applications and information in the system from accidental or malicious alteration or destruction and provide assurance to users that data has not been altered. An example of this is message authentication. Information and guidelines on operating system controls and system administration procedures are normally described in vendor supplied documentation. This information should be made available to users and adhered to. Local SOPs should reflect the guidance and procedures for integrity controls.

d. Audit Trail Mechanisms (3c.5.D). Audit trail mechanisms provide a system monitoring and recording capability to retain a chronological record of system activities. Such controls normally enable the reconstruction of system activity. The use of system log files is an example of this type of control. Procedures and guidelines should be reflected in the local SOPs.

e. Confidentiality Controls (3c.5.E). Confidentiality controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. These

controls may provide data protection at the user site, at a computer facility, in transit, or some combination of these. An example of this is encryption. IRM-5239-08, Computer Security Procedures, IRM-5239-10, Small Computer Systems Security, and local SOPs provide the guidance and procedures for confidentiality.

4.4.6. Controls Over the Security of Applications (3c.6). The security of each application that is processed on a GSS affects the security of all others types of processing. Thus, the manager of the support system should understand the risk that each application represents to the system. If not, plans for greater understanding of that risk should be described. An example of this is the access to programming capabilities for application users. This represents a higher risk to the support system than when they were confined to individual application functions. Similarly, applications that utilize dial-up communications represent a higher risk to the system than those that prohibit dial-up functions. Local SOPs should address this control.

4.5. GUIDANCE AND REFERENCES (3d). List all references and documents that provide guidance and instructions for the security control measures. Examples of guidance and references are Government Directives, Marine Corps Orders and technical publications, and standing operating procedures. These references and documents should be made available in the event of an audit or inspection.

4.6. SUPPORTING DOCUMENTATION (3e). List all documents and forms, required by the references and guidance, that must be maintained and updated in support of the security control measures. Examples include investigation forms, accreditation plans and contingency of operation plans.

4.7. SECURITY CONTROL MEASURE STATUS (3f). Each security control measure listed must have an appropriate status. The Security Control Measure Status is made up of three parts. The SCM which identifies the security control measure, the actual status code and the date of implementation or pending implementation. Figure 4-02 contains examples of the status for security control measures.

Security Control Measures:	SCM	Status Code:	Date (YY/MM/DD):
(1) Management Controls:			
(a) Assignment of Security Resp	a	P	900911
(b) Personnel Screening	b	I	901015
(c) Risk Analysis	c	IP	901201

Figure 4-02
Example of Security Control Measures Status

The following are the security control measure status codes.

a. I = In Place - Control measures listed are in place and operational and judged to be effective. Indicate the effective date of implementation.

b. P = Planned - Control measures (new, enhanced) are planned for the system. Indicate a general description of the planned measures and their expected operational dates. Identify any interim measure being taken, if applicable.

c. IP = In Place and Planned - Some measures are in place, while others are planned. A general description of the planned measures and expected operational dates should be provided.

d. NA = Not Applicable - This type of control measure is not needed, cost-effective, or appropriate for this system.

4.8. ADDITIONAL COMMENTS (4). The final section of the SSP is intended to provide an opportunity to include additional comments about the security of the subject system and any perceived need for guidance, standards or further security explanations.

(This page intentionally left blank)

Appendix A

PUBLIC LAW 100-235
COMPUTER SECURITY ACT OF 1987

A brief summary of the Computer Security Act of 1987 is provided for your convenience. The Act, in its entirety, follows this summary.

SUMMARY: The Computer Security Act of 1987 amends several laws to add provisions relating to the protection of computer-related assets (e.g., hardware, software, and data). The Act -

- Assigns responsibility for the development of computer security guidelines and standards to the National Institute of Standards and Technology (NIST);

- Requires that within 6 months after the enactment of the Act, Federal agencies identify existing systems and systems under development that contain sensitive information;

- Requires development of a security plan for each identified sensitive computer system within 1 year of enactment of the Act; and

- Requires mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of Federal computer systems.

GENERAL:

To provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987".

SECTION 2. PURPOSE.

(a) In General - The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) Specific Purposes - The purposes of this Act are:

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SECTION 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended -

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu of thereof: ";and", and by inserting after such paragraph the following: "(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

(2) By redesignating section 20 as section 22, and by inserting after section 19 the following sections:

Sec 20. (a) The National Bureau of Standards shall -

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except -

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy, the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant of paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

Sec 20. (b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized -

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

(4) to assist, appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to

devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)-

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense of foreign policy.

Sec 20. (c) For the purpose of -

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection (b)(5), the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

Sec 20. (d) As used in this section -

(1) the term 'computer system' -

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes -
- (i) computers;
- (ii) ancillary equipment;
- (iii) software, firmware, and similar procedures;
- (iv) services, including support services; and
- (v) related resources as defined by regulations issued by the Administrator for General

Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

(2) the term 'Federal computer system' -

(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest of the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

Sec 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer

system security and privacy, at least one of whom shall be from the National Security Agency.

Sec 21. (b) The duties of the Board shall be -

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

Sec 21. (c) The term of office of each member of the Board shall be four years, except that -

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

Sec 21. (d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

Sec 21. (e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

Sec 21. (f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

Sec 21. (g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act; and

(3) by adding at the end thereof the following new section: "Sec 23. This Act may be cited as the National Bureau of Standards Act".

SECTION 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows

(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United STates Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch 201) to be consistent

with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SECTION 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) In General - Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be -

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) Training Objectives - Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed -

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) Regulations - Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SECTION 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) Identification of Systems That Contain Sensitive Information - Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under he supervision of that agency and which contains sensitive information.

(b) Security Plan - Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

SECTION 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal Computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

SECTION 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed -

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is -

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

(This page intentionally left blank)

Appendix B

REFERENCES

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

2. OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information.

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

4. Public Law 93-503, Freedom of Information Act.

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

6. Public Law 97-255, Federal Managers Financial Integrity Act of 1982.

7. Public Law 99-474, Computer Fraud and Abuse Act of 1986.

8. DoD Directive 5200.28, Security Requirements for AISs.

9. SECNAVINST 5239.2, DON AIS Security Program.

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

11. OPNAVINST 5239.1A, DON ADP Security Program.

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

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

14. MCO 5271.1, IRM Standards and Guidelines Program.

(This page intentionally left blank)

Appendix C

TERMS AND DEFINITIONS

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

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 the 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.

AIS: Automated Information System

Audit: To conduct an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail: A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in the path of a transaction from its inception to output of final results.

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

Availability: This refers to the protection requirement to provide service as needed for a system that contains information that without this availability could erode the quality and accuracy of the information necessary an organization's overall mission.

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.

Class I: An AIS that is sponsored by a HQMC functional manager and provides Marine Corps-wide support. The following subclassifications are provided to define the processing environment and autonomy of the AIS:

Class IA: A Class I AIS that supports the data input and output functions of a parent Class IB system (i.e., a Class IA acts as a feeder system to a Class IB system), provides Marine Corps-wide support, and is processed on small workspace computers organic to the supporting establishment and/or the FMF.

Class IB: A Class I AIS that operates on a mainframe computer.

Class IC: A stand-alone AIS that provides Marine Corps-wide support and is processed on small workspace computers organic to the supporting establishment and/or the FMF. Class IC systems have no parent Class IB applications.

Class II: An AIS that supports the local needs of a HQMC staff agency, an FMF unit, or a supporting establishment organization. The following subclassifications are provided to define the processing environment and autonomy of the AIS:

Class IIA: A Class II Ais that supports the data input and output functions of a parent Class IIB system (i.e., a Class IIA acts as a feeder system to a Class IIB system) and is processed on small workspace computers organic to the supporting establishment and/or the FMF.

Class IIB: A Class II AIS that operates on a mainframe computer.

Class IIC: A stand-alone AIS that supports the local needs of a HQMC staff agency, an FMF command, or a supporting establishment organization and is processed on small workspace computers organic to the supporting establishment and/or the FMF. Class IIC systems have no parent Class IIB application.

Class III: An AIS that supports a HQMC staff agency, an FMF unit, or a supporting establishment organization and is sponsored by a Government agency external to the Marine Corps. The implementation of the AIS is mandated by higher headquarters. The following subclassifications are provided to define the processing environment and autonomy of the AIS:

Class IIIA: A Class III AIS that supports the data input and output functions of a parent Class IIIB system (i.e., a Class IIIA acts as a feeder station to a Class IIIB system) and is processed on small workspace computers organic to the supporting establishment and/or the FMF.

Class IIIB: A Class III AIS that operates on a mainframe computer.

Class IIIC: A stand-alone Class III AIS that supports a HQMC staff agency, an FMF unit, or a supporting establishment organization; that is sponsored by a Government agency external to the Marine Corps; and is processed on small workspace

computers organic to the supporting establishment and/or the FMF. Class IIIC systems have no parent Class IIIB application.

Cluster of Small Computers: Small computers located in close proximity, 2 to 25 in number, same classification of data, similar hardware, software, configuration and purpose.

Component: Individual sections to the System Security Plan. There are four components: Basic System Identification, Sensitivity of Information Handled, System Security Measures, and Additional Comments/Guidance.

Computer Systems Security Officer (CSSO): CSSOs are responsible for the effective implementation of computer security regulations. These regulations are meant to ensure that the security needs of all functional sponsors are met and to resolve any conflicts between systems. Further, they ensure that the computer activities do not compromise their functional sponsor's data while acting as the sponsor's resource custodian. CSSOs should report directly to the head of the organization.

Confidentiality: This refers to the unauthorized disclosure protection requirement for a system that contains information that could compromise or become detrimental to an organization's overall mission.

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. A contingency plan is synonymous with a disaster plan and an emergency plan.

CSSO: Computer System Security Officer

DAA: Designated Approval Authority
Dedicated Security Mode: A mode of operation wherein all users have the clearance, formal access approval, and need-to-know for all data handled by the AIS. 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.

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

General Support System (GSS): All computer systems that are not classified or considered as Major Application(AIS). GSS provide such functions as word processing, database management, and general information processing in support of a local command or organization.

Information Systems Management Officer (ISMO): The ISMO is the primary staff officer for information resource matters within an FMF or Supporting Establishment command.

Integrity: This refers to the system that contains information which must be protected from unauthorized, unanticipated, or unintentional modification which would jeopardize the system's information reliability.

IRM: Information Resource Management

LAN: Local Area Network

LCM: Life Cycle Management

LCM-AIS: Life Cycle Management for Automated Information Systems

Level of Protection: This refers the extent in which the sensitive information is to be protected. There are three levels of protection for the SSP: Primary, Secondary, and Minimal.

Life Cycle Management (LCM): A management discipline for acquiring and using AIS resources in a cost-effective manner throughout the entire life of an AIS.

Major Application(AIS): A major application is synonymous with AIS. A combination of information, computer, and telecommunications resources, and other information technology and personnel resources which collects, records, processes, stores, communicates, retrieves, and displays information.

Mid-Range Information Systems Plan (MRISP): An AIS tracking tool which describes the information resource needs for Marine Corps AISs, both operational and in the development stages, and reflects the strategic planning effort in an annually updated document.

MRISP: Mid-Range Information Systems Plan

National Interest Data: Any information of which the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest of the conduct of Federal programs.

Operational Control: (DoD) The authority delegated to a commander to perform those functions of command involving the assignment of tasks, the designation of objectives, and the authoritative direction necessary to accomplish the mission.

Privacy Data: Information that is personal in nature and is protected specifically under the Privacy Act of 1974.

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

Risk Assessment: The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

Risk Management: The total process of identifying, controlling, and minimizing uncertain events affecting AIS resources. it includes risk analysis, cost benefit analysis, selection of safeguards, security test and evaluation, safeguard implementation, and system review.

Security Level: The combination of a hierarchal classification and a set of non-hierarchal categories that represents the sensitivity of information.

Security Mode: A secure mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the security modes(dedicated, system high, multilevel, 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.

Sensitive Unclassified Information: Any information, the loss, misuse, modification of, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code (The Privacy Act).

SSP: System Security Plan

ST&E: Security Test and Evaluation

System Security Plan: An organized attempt to identify computer system vulnerabilities and their impact on the organization supported by the information stored or processed on that computer. The SSP is a set of instructions, guidelines and measures that are essential in the safeguarding of the information processed or stored on the computer system.

TASO: Terminal Area Security Officer

Terminal Area Security Officer (TASO): TASOs must be appointed by each commanding general or officer, directors and officer-in-charge who has individuals in his/her organization with a requirement to use a Major Application(AIS), General Support System or network. TASOs must ensure that each terminal user's

need-to-know, level of clearance (where appropriate), and access authorizations are established commensurate with the data the user can obtain from terminals to which access is authorized.

Trusted Computer System: This is 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.

User: A user is an organization or individual having a valid requirement to use a system or its output. The user may specify the need for the development or modification of the system, participate in system design, or utilize the computer and its resources as a tool within day-to-day events.

Appendix D

CROSS REFERENCES TO EXISTING SECURITY PUBLICATIONS

1. **COMPUTER SECURITY BASICS:**

OMB Circular A-130, "Management of Federal Information Resources"

Privacy Act of 1974, P.L. 93-579

Computer Fraud and Abuse Act of 1986, P.L. 99-474

Computer Security Act of 1987, P.L. 100-235

Computer Crime: Electronic Fund Transfer Systems and Crime, U.S. Department of Justice

Computer Crime: Legislative Resource Manual, U.S. Department of Justice

FIPS PUB 39, "Glossary for Computer Systems Security"

FIPS PUB 112, "Standard on Password Usage"

NBS Special PUB 500-120, "Guide to Auditing for Controls and Security - A Management Guide"

NBS Special PUB 500-153, "Guide to Auditing for Controls and Security - A System Development Life Cycle Approach"

NIST Special PUB 500-166, "Computer Viruses and Related Threats - A Management Guide"

2. **COMPUTER SECURITY PLANNING AND MANAGEMENT:**

OMB Circular No. A-123, "Internal Control Systems"

OMB Circular No. A-127, "Financial Management Systems"

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

OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information"

FIPS PUB 31, "Guidelines for ADP Security Risk and Management"

FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974"

FIPS PUB 65, "Guideline for Automatic Data Processing Risk

Analysis"

FIPS PUB 73, "Guidelines for Security of Computer Applications"

FIPS PUB 94, "Guidelines on Electrical Power for ADP Installations"

NBS Special PUB 500-25, "An Analysis of Computer Security Safeguards for Detection and Prevention of Intentional Computer Misuse"

NBS Special PUB 500-33, "Consideration in the Selection of Security Measures of Automatic Data Processing Systems"

NBS Special PUB 500-57, "Evaluation of Computer Security"

NBS Special PUB 500-109, "Overview of Computer Certification and Accreditation"

NBS Special PUB 500-120, "Security of Personnel Computer Systems - A Management Guide"

NBS Special PUB 500-133, "Technology Assessment: Methods for Measuring the Level of Computer Security"

NBS Special PUB 500-153, "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach"

NIST Special PUB 500-166, "Computer Viruses and Related Threats: A Management Guide

NIST Special PUB 500-169, "Executive Guide to the Protection of Information Resources"

NIST Special PUB 500-170, "Management Guide to the Protection of Information Resources"

NIST Special PUB 500-171, "Computer User's Guide to the Protection of Information Resources"

NIST Special PUB 500-172, "Computer Security Training Guidelines"

NIST Special PUB 500-174, "Guide for Selecting Automated Risk Analysis Tools"

NBSIR 86, "Work Priority Scheme for EDP Audit and Computer Security Review"

OPM 5 CFR PART 930, "Training Requirements for the Computer Security Act"

3. **COMPUTER SECURITY POLICIES AND PROCEDURES:**

Privacy Act of 1974, P.L. 93-579

Federal Manager's Financial Integrity Act of 1982, P.L. 97-255

Computer Fraud and Abuse Act of 1986, P.L. 99-474

Electronic Communications Privacy Act, P.L. 99-508

Computer Security Act 1987, P.L. 100-235

OMB Circular No. A-123, "Internal Control Systems"

OMB Circular No. A-127, "Financial Management Systems"

OMB Circular No, A-130, "Management of Federal Information Resources"

FIPS PUB 39, "Glossary for Computer Systems Security"

FIPS PUB 46-1, "Data Encryption Standard"

FIPS PUB 48, "Guidelines in Evaluation of Techniques for Automated Personnel Identification"

FIPS PUB 74, "Guideline for Implementing and Using the NBS Data Encryption Standard"

FIPS PUB 81, "DES Modes of Operation"

FIPS PUB 112, "Standard on Password Usage"

FIPS PUB 113, "Standard on Computer Data Authentication"

NBS Publication List 58, "Federal Information Processing Standards Publications (FIPS PUBs) Index"

NBS Publication List 88, "Computer Science and Technology Publications"

NBS Publication List 91, "Computer Security Publications"

NBS Special PUB 500-61, "Maintenance Testing for the Data Encryption Standard"

NBS Special PUB 500-120, "Security of Personal Computer Systems - A Management Guide"
NBS Special PUB 500-121, "Guidance on Planning and Implementing Computer Systems Reliability"

NBS Special PUB 500-133, "Technology Assessment Methods for Measuring the Level of Computer Security"

NIST Special PUB 500-174, "Guide for Selecting Automated Risk Analysis Tools"

4. **CONTINGENCY PLANNING:**

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

Federal Personnel Manual Chapter 732, "Personnel Security"

NBS Special PUB 500-85, "Executive Guide to ADP Contingency Planning"

NBS Special PUB 500-134, "Guide on Selecting ADP Backup"

NBS Special PUB 500-156, "Message Authentication Code (MAC) Validation System: Requirements and Procedures"

NBS Special PUB 500-157, "Smart Card Technology: New Methods for Computer Access Control"

NIST Special PUB 500-166, "Computer Viruses and Related Threats - A Management Guide"

IRM-5233-01, "Computer Facility Management" (to be published)

5. **COMPUTER SYSTEMS LIFE CYCLE MANAGEMENT:**

OMB Circular No. A-123, "Internal Control Systems"

OMB Circular No. A-127, "Financial Management Systems"

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

GAO, "Policy and Procedures Manual for Guidance of Federal Agencies, Title II Accounting"

GSA Federal Information Resource Management Regulation (FIRMR), Part 201-30-007, "Determination of Need and Requirements Analysis"

FIPS PUB 38, "Guidelines for Documentation of Computer Programs and Automated Data Systems"

FIPS PUB 64, "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase"

6. **MARINE CORPS SYSTEM DEVELOPMENT METHODOLOGY (SDM) PUBLICATIONS (for Major Applications(AIS)):**

5231-01, "SDM Overview"

5231-02A, "SDM Developer Perspective"

5231-04, "Functional Requirements Definition" (s)(d)

5231-05, "General Design Specification" (s)(d)

5231-06, "Detailed Design Specification" (s)(d)

5231-07, "User's Manual", (s)(d)

5231-08A, "Computer Operations Manual" (s)(d)

5231-09A, "Application Configuration Management Plan (d)

5231-10, "Quality Assurance Plan" (d)

5231-11, "Data Base Plan" (d)

5231-12, "ADPE Support Plan" (d)

5231-13, "Data Base Conversion Plan" (d)

5231-14, "Test Plan" (d)

5231-15, "Training Support Plan" (d)

5231-16, "Implementation Plan" (d)

5231-17, "Inspection and Acceptance"

5231-18, "Prototyping Standard"

5231-19A, "Project Management Plan" (d)

5231-20A, "Requirements Statement" (s)(d)

5231-21, "AIS Project Baselining" (d)

5236-03, "Economic Analysis" (s)(d)

5239-05, "Telecommunications Support Plan" (d)

5239-13, "System Security Plan" (d)

7. **MARINE CORPS COMPUTER SECURITY TECHNICAL PUBLICATIONS:**

IRM-5239-06, "Data Access Security"

IRM-5239-07, "Terminal Area Security Officer (TASO)"

IRM-5239-08, "Computer Security Procedures"

IRM-5239-09, "Contingency Planning"

IRM-5239-10, "Small Computer Systems Security"

IRM-5239-11, "Accreditation Process" (to be published)

IRM-5239-12, "Project Manager's Security Handbook"

IRM-5239-13, "System Security Plan"

8. **ORDERING INFORMATION:**

NBS Publication List 58, "Federal Information Processing Standards Publications (FIPS PUBs) Index"

> Available from the **NATIONAL TECHNICAL INFORMATION SERVICE**, 5285 Port Royal Road, Springfield, VA., 22161; (703) 487-4650

NBS Publication List 88, "Computer Science and Technology Publications"

> Available from the **NATIONAL TECHNICAL INFORMATION SERVICE**, 5285 Port Royal Road, Springfield, VA., 22161; (703) 487-4650

Marine Corps IRM Technical Publications are available in small quantities (up to 10) by completing a DD 1348 and submitting it to the Marine Corps Stock Order Point, MCLB, Albany, GA., 31704-5065, IAW MC P4400.84C, Ch. 11.

(s) = Specifications
(d) = Documentation

Appendix E

SSP BLANK WORKSHEETS

1. GENERAL. The following pages contain SSP blank worksheets that have been created for your convenience. These worksheets were designed to coincide with chapters 2 through 4 of this publication. These worksheets can be duplicated, modified and tailored to meet the organization's SSP requirements. However, if you do modify the worksheets, ensure that the required information, as identified in this technical publication, is included. Each page is identified as either a Major Application(AIS) or General Support System (GSS). Ensure the correct pages are used for the appropriate type system.

(This page intentionally left blank)

SYSTEM SECURITY PLAN (SSP)

1. BASIC SYSTEM IDENTIFICATION – Major Application(AIS)

Page ____ of ____

a. Responsible Organization:

_____
(Functional Manager)

b. System Name/Title:

c. System Category

[X] AIS
[ ] Class I
[ ] Class II
[ ] Class III

d. Processing Location:

_____

Data Input Location:

_____

[ ] Locations are identified on Continuation of Basic System Identification (Page ___)

e. System Operational Status:

[ ] Operational [ ] Under Development

f. General Description/Purpose:

g. System Environment and Special Considerations:

h. Information Contacts:

NAME	TITLE	ORGANIZATION ADDRESS	PHONE: AV	COMM

2. SENSITIVITY OF INFORMATION HANDLED – Major Application(AIS)

a. General Description of Information Sensitivity:

Information Category (MRISP Code):

Privacy 1 – 7 [P ___] or National 1 – 13 [N ___]

b. System Classification:

- ☐ Sensitive Unclassified
- ☐ OTHER (_____)

c. Applicable Laws or Regulations Affecting the System:

(d) Protection Requirement:	(e) Level of Protection
(1) CONFIDENTIALITY:	☐ Primary (P) ☐ Secondary (S) ☐ Minimal (M) MRISP Code [C ___]
(2) INTEGRITY:	☐ Primary (P) ☐ Secondary (S) ☐ Minimal (M) MRISP Code [I ___]
(3) AVAILABILITY:	☐ Primary (P) ☐ Secondary (S) ☐ Minimal (M) MRISP Code [A ___]

3. SYSTEM SECURITY MEASURES – MAJOR APPLICATION(AIS)

Page ____of_____

a. Risk Analysis Method: ☐ Formal ☐ Other

b. Name:

c. Security Control Measures:	d. Guidance and References	e. Supporting Documentation	f. Status SCM	Code	Date
(1) Management Controls:			(a)		
(A) Assignment of Security Responsibilities			(b)		
(B) Personnel Screening					
(2) Development/Implementation Controls			(a)		
(A) Security Specifications			(b)		
(B) Design Review and Testing			(c)		
(C) Certification			(d)		
(D) ST&E			(e)		
(E) Risk Assessment					
(3) Operational Controls:			(a)		
(A) Physical and Environment Protection			(b)		
(B) Production, I/O Controls			(c)		
(C) Emergency, Back-up, Contingency Planning			(d)		
(D) Audit and Variance Detection			(e)		
(E) Documentation			(f)		
(F) Application SW Maintenance Controls			(g)		
(G) HW/System SW Maintenance Controls					
(4) Security Awareness/Training Measures			(a)		
(A) Program/Activities					
(5) TECHNICAL CONTROLS:			(a)		
(A) User Identification/Authentification			(b)		
(B) Authorization/Access Controls			(c)		
(C) Data Integrity/Validity Controls			(d)		
(D) Audit Trails and Journeling					

3. SYSTEM SECURITY MEASURES -- MAJOR APPLICATION(AIS) (Cont.)

c. Security Control Measures:	d. Guidance and References	e. Supporting Documentation	f. Status SCM	Code	Date
(6) Complementary Controls Provided by support Systems					

4. ADDITIONAL COMMENTS

CONTINUATION OF BASIC SYSTEM IDENTIFICATION – MAJOR APPLICATIONS(AIS)

Page ___ OF ___

MAKE	MODEL	LOCATION	STATUS

SYSTEM SECURITY PLAN (SSP)

1. BASIC SYSTEM IDENTIFICATION – General Support System (GSS)

Page ____ of ____

a. Responsible Organization:

b. System Name/Title:

c. System Category:

☐ LAN

☐ Cluster of Small Computers

☐ Stand Alone Small Computer

d. ☐ Make/Model/Serial #/Location:

_____

_____

☐ Location and information are listed on Continuation of Basic System Identification (Page ___)

☐ HW/SW Inventory Attached

e. System Operational Status:

☐ Operational ☐ Under Development

f. General Description/Purpose:

g. System Environment and Special Considerations:

h. Information Contacts:

NAME	TITLE	ORGANIZATION ADDRESS	PHONE: AV	COMM

2. SENSITIVITY OF INFORMATION HANDLED – General Support System (GSS)

a. General Description of Information Sensitivity:

Privacy 1 – 7: P ____ or National 1 – 13: N ____ or Not Applicable: NA ____

b. System Classification:

- ☐ Sensitive Unclassified
- ☐ OTHER (_____)

c. Applicable Laws or Regulations Affecting the System:

(d) Protection Requirement:	(e) Level of Protection
(1) CONFIDENTIALITY:	☐ Primary (P) ☐ Secondary (S) ☐ Minimal (M) C ____
(2) INTEGRITY:	☐ Primary (P) ☐ Secondary (S) ☐ Minimal (M) I ____
(3) AVAILABILITY:	☐ Primary (P) ☐ Secondary (S) ☐ Minimal (M) A ____

CONTINUATION OF BASIC SYSTEM IDENTIFICATION – GENERAL SUPPORT SYSTEM (GSS)

Page ___ OF ___

MAKE	MODEL	SERIAL NUMBER	LOCATION	STATUS

3. SYSTEM SECURITY MEASURES – GENERAL SUPPORT SYSTEM (GSS)

a. Risk Analysis Method: ☐ Formal ☐ Other | (b). Name:

c. Security Control Measures:	d. Guidance and References	e. Supporting Documentation	f. Status SCM Code	Date
(1) Management Controls: (A) Assignment of Security Responsibilities (B) Personnel Screening (C) Risk Analysis			(A) (B) (C)	
(2) Acquisition/Development/Installation Ctls (A) Acquisition Specifications (B) Accreditation (C) Certification			(A) (B) (C)	
(3) Operational Controls: (A) Physical and Environment Protection (B) Production, I/O Controls (C) Emergency, Back-up, Contingency Planning (D) Audit and Variance Detection (E) HW and System SW Maintenance Controls (F) Documentation			(A) (B) (C) (D) (E) (F)	
(4) Security Awareness/Training Measures: (A) Security Awareness and Training Measures			(A)	
(5) TECHNICAL CONTROLS: (A) User Identification/Authentification (B) Authorization/Access Controls (C) Integrity Controls (D) Audit Trails Mechanisms (E) Confidentiality Controls			(A) (B) (C) (D) (E)	
(6) Controls Over The Security of Applications:				