IRM-5230-01A

U.S. Marine Corps

FMF-EUCE AUTOMATED INFORMATION SYSTEM (AIS) GUIDELINES

UNITED STATES MARINE CORPS
MARINE CORPS COMPUTER AND TELECOMMUNICATIONS ACTIVITY
QUANTICO, VIRGINIA 22134-5010

From: Director, Marine Corps Computer and Telecommunications Activity

Subj: FLEET MARINE FORCE-END USER COMPUTING EQUIPMENT (FMF-EUCE) AUTOMATED INFORMATION SYSTEMS (AIS) GUIDELINES

Ref: (a) MCO 5271.1
        (b) AN/UYK-83 and AN/UYK-85 Material Fielding Plan (MFP)

Encl: (1) IRM-5230-01A

1.   PURPOSE.   To provide standards and guidance on the management of Automated Information Systems (AIS's) that operate on the Fleet Marine Force - End User Computing Equipment (FMF-EUCE).

2.   CANCELLATION.   IRM-5230-01

3.   AUTHORITY.   This publication is published under the auspices of reference (a).

4.   APPLICABILITY.   The guidance contained in this publication is applicable to all Marine Corps personnel and contractors responsible for the design, development, implementation and operation of AIS's that are processed on the FMF-EUCE. This publication supplements information contained in reference (b). This standard is applicable to the Marine Corps Reserve.

5.   SCOPE

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

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

6.   RECOMMENDATIONS.   Recommendations concerning the contents of this technical publication should be forwarded via the appropriate chain of command to Director, MCCTA, at the following address:

              United States Marine Corps
              MARCORCOMTELACT
              (CTAS)
              3255 Myers Ave
              Quantico VA   22134-5048

       MARCORCOMTELACT QUANTICO VA OMB   (GICIZZ:MQGMCCTA)

Subj: FLEET MARINE FORCE-END USER COMPUTING EQUIPMENT (FMF-EUCE)
        AUTOMATED INFORMATION SYSTEMS (AIS) GUIDELINES

7. SPONSOR. The sponsor of the technical publication is CMC
(MCCTA).

D. P. HOUSTON
Colonel, U.S. Marine Corps
Director, Marine Corps
Computer and
Telecommunications Activity

DISTRIBUTION: PCN 186 523001 00

Copy to: 8145001

UNITED STATES MARINE CORPS

Information Resources Management (IRM) Standards
and Guidelines Program

<u>FMF-EUCE Automated Information Systems (AIS) GUIDELINES</u>
IRM-5230-01A

(This page intentionally left blank)

TECHNICAL PUBLICATION LIBRARY MAINTENANCE

The Information Resources Management Standards and Guidelines Program will be maintained at each receiving activity. Each activity is responsible for ensuring that their set of technical publications is complete, and that all published changes are promptly incorporated.

RECORD OF CHANGES

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 5

DATA COMMUNICATIONS

APPENDICES

(This page intentionally left blank)

LIST OF FIGURES

(This page intentionally left blank)

Chapter Table of Contents

Chapter 1

GENERAL

(This page intentionally left blank)

Chapter 1

GENERAL

1.1. PURPOSE. This Technical Publication is intended primarily
for personnel serving as Information Systems Management Officers
(ISMO's) and addresses procedures for the Automated Information
Systems (AIS's) that will operate on the Fleet Marine Force - End
User Computing Equipment (FMF-EUCE). This publication
supplements other documents necessary for implementation and
support to include the Material Fielding Plan (MFP), the Combined
User and Computer Operation Manual, and the Interim Maintenance
Manual.

1.2. BACKGROUND. The FMF-EUCE is currently configured in two
sizes: A full sized desktop computer (AN/UYK-83) and a Down-sized
End User Computing Device (DEUCE) (AN/UYK-85). The number
following the AN/UYK designation refers to the chassis size. The
FMF-EUCE is available with three different central processing
units (CPUs). The AN/UYK-83 and AN/UYK-85 have 80286-based CPUs,
the AN/UYK-83A has an 80386-based CPU, and the AN/UYK-85A has an
80486-based CPU.

1.2.1. Current Situation. The FMF-EUCE devices will be used to
process AIS's which support such functions as personnel, pay,
supply, maintenance, embarkation, command and control, and
intelligence as well as local applications. This equipment
replaced the 842 Automatic Data Processing Equipment for the
Fleet Marine Force (ADPE-FMF) minicomputers (also known as Green
Machines). The FMF-EUCE is provided to the Fleet Marine Force at
the battalion and squadron level and provides a standard suite of
equipment and software for FMF units. The equipment is
ruggedized to withstand heat, humidity, dust, sand, shock, and
vibration. It also meets Electromagnetic Interference (EMI) and
TEMPEST requirements.

1.2.2. Standardization. The joint service contract for Zenith
Z-248 microcomputers afforded the Marine Corps an opportunity to
standardize the Supporting Establishment (SE) microcomputer
environment but did not meet the requirements of the FMF
commander when deployed. The FMF-EUCE Program provides the FMF
commander with a TEMPEST accredited system that is ruggedized for
operation in a deployed environment, standardizes the FMF's
microcomputer environment, is compatible with the Zenith Z-248
microcomputer in the Supporting Establishment, and provides the
computing capacity to support the current information processing
requirements as well as identified requirements for future
growth.

1.2.3. Supportability. Supportability is enhanced by the level
of ruggedization plus the option of using either contractor
maintenance or organic maintenance provided by the Force Service

Support Groups' (FSSG's) Electronic Maintenance Companies
(ELMACO's). Training, spare parts, and provisioning have been
included in the contract to support the FMF-EUCE organic
maintenance option. Also, the FMF-EUCE is a Table of Equipment
(T/E) item and as such will be managed and accounted for in the
same manner as any other T/E item. The Marine Corps Systems
Command is responsible for fielding the FMF-EUCE.

Chapter Table of Contents

Chapter 2

FMF-EUCE CONCEPT OF OPERATIONS

(This page intentionally left blank)

Chapter 2

FMF-EUCE CONCEPT OF OPERATIONS

2.1. GENERAL. The concept of operation for providing data
processing support is structured around centralized policy
formulation, technical direction, and acquisition under the AC/S
C4I. This concept also includes centralized development and
maintenance of standard AIS's, and decentralized processing of
AIS's by regional services centers while in garrison or by
various deployable information resources such as the FMF-EUCE, or
the Force Automated Services Centers (FASCs) while in a deployed
or combat environment. AIS management responsibilities are
outlined in MCO P5231.1. Responsibilities and functional
relationships are detailed in this chapter.·

2.2. GARRISON SUPPORT. The concept of operation while in
garrison is to provide data processing support through the
established command structure and a hierarchy of regional
services centers. The centers are interconnected by MCDN and
include the Marine Corps Computer and Telecommunications Activity
(MCCTA, Quantico), the Information Resource Management
Directorate (IRMD, Albany), the Defense Information Technology
Services Organization-Kansas City Center (DITSO-KC), and Regional
Automated Services Centers (RASCs). In accordance with the
current edition of MCO P5230.2, certain centers are organized,
staffed, and equipped to analyze, design, develop, program, test,
implement, and maintain Class I AIS's that are processed on the
FMF-EUCE. These designated centers act as systems sponsors for
assigned software products, providing detailed technical
guidance, management, and control for those products. The
Technical Support Division, MCCTA sponsors the system software
that operates on the FMF-EUCE. In addition, remote job entry
(RJE) facilities provide access to the regional services centers
at selected locations. FMF-EUCE serves as a Source Data
Automation (SDA) tool for Class IA AIS's as well as a processing
tool for stand-alone Class IC AIS's.

2.2.1. Regional Automated Services Centers (RASC's). Currently,
the three RASC's are located at Marine Corps Base (MCB) Camp
Lejeune, North Carolina; MCB Camp Pendleton, California; and Camp
Kinser, Okinawa, Japan. RASC's provide data processing support
to the supporting establishment and FMF commands within their
regions in accordance with the current edition of MCO 5230.13.
Accordingly, these sites and their respective Remote Job Entry
(RJE) sites support data aggregation and diskette duplication for
FMF-EUCE.

2.2.2. Remote Job Entry (RJE) Facilities. The RJE facilities
are under the operational control of the commanding
general/officer of the base or station where they are located,
or, in some cases, under the operational control of the connected

RASC. The primary functions of an RJE facility are to provide day-to-day AIS production support, limited programming, and troubleshooting services for interactive terminals at the supported activity or base. FMF units in garrison utilize RJE facilities to input their Class IA to parent Class I AIS's.

2.2.3. <u>Information Systems Management Officer (ISMO)</u>. The ISMO is the primary staff officer for information resource matters within an FMF command. In a deployed environment, the ISMO is the command focal point for all matters pertaining to AIS matters as outlined in para 2.2.4. This is true whether the FMF is in or out of the garrison environment. According to FMFM 3-1, the ISMO's functions include:

a. Advising the commander and his staff on information technology matters.

b. Acting as the command focal point on all matters pertaining to coordination of information technology requirements, objectives, concepts, plans and policies, including establishing priorities with supporting and external data processing activities.

c. Exercising staff supervision of organic data processing units and equipment. This includes the FMF-EUCE.

d. Preparing IRM support estimates, operating and contingency plans, and ensuring that these items are tested.

2.2.4. <u>Marine Corps Data Network (MCDN)</u>. The MCDN is a common-user data communications network which provides terminal-to-computer and computer-to-computer communications for FMF and SE units in garrison. The MCDN architecture is based on the use of communications processors as the major nodal elements in the network. The communications processors perform front end processing for all host computers, switching/line control for all terminals, and other network communications functions. Connectivity between nodal points is provided by leased circuits. MCDN will be used for all AIS's for the SE and the FMF while in garrison. Terminals and other devices gain access to the MCDN primarily through dedicated circuits to the nearest nodal point. All terminals connected to the network can access any host computer in the network in an on-line interactive mode. The FMF-EUCE can be used as a terminal when properly configured. Access to MCDN is also available through the 3270 option of a unit's LAN.

2.3. <u>DEPLOYED SUPPORT</u>. To support deployed FMF units, the Marine Corps has fielded the FMF-EUCE ruggedized microcomputers which provide organic data processing support down to the battalion/squadron and separate company level. This program enables the local commander to more efficiently provide input to Class I AIS's such as JUMPS/MMS, SASSY, and MIMMS. Unit

commanders are also able to develop and share local applications to improve local management functions.

2.3.1. <u>Deployable Force Automated Services Center (DFASC)</u>. The capabilities of the DFASC, located at MCCTA Quantico, VA, will be retained to support each Marine Expeditionary Force (MEF) as a deployment contingency as required. Current capabilities of the DFASC consist of a portable mainframe computer with high speed data storage, print, and communications equipment contained within a tactical semi-trailer capable of being deployed by air, sea, truck or rail in support of deployed operations or combat. The DFASC is capable of interfacing with PC based systems or processing Class I AIS's for a MEF or MEF (+) sized force.

2.4. <u>RESPONSIBILITIES</u>. (In relation to FMF-EUCE)

2.4.1. <u>Users</u>. A user is an individual or any command, staff, or operational element which uses the FMF-EUCE device. The responsibility of the user is to maintain the FMF-EUCE device as the target device for processing of Class IA and Class IC AIS's. Users will direct all issues pertaining to the FMF-EUCE through their normal chain of command to the appropriate command designated representative, as established by local policy.

2.4.2. <u>Supply Officers</u>. ADPE has traditionally been managed differently than other property. Due to the proliferation of end user computing equipment and the mission critical nature of the FMF-EUCE, however, it is neither practical nor prudent to manage the receipt, accounting, issuance, and maintenance of the FMF-EUCE without using the existing supply structure and procedures. The unit supply officer is normally the point of contact for these functions. The FMF-EUCE is issued to units as a Table of Equipment (T/E) item.

2.4.3. <u>Commanding Officers</u>. The commanding officer is responsible for implementing command procedures regarding the use of FMF-EUCE and following policy established by Headquarters Marine Corps functional managers for the operation of Class IA and Class IC AIS's.

2.4.4. <u>Information Systems Management Officers (ISMO's)</u>. Marine Expeditionary Force (MEF), Force Service Support Group (FSSG), Division, Wing, and Brigade ISMO's are the primary staff officers within their respective commands for technical FMF-EUCE matters as established in FMFM 3-1 and FMFM 4-1. The ISMO is responsible for the technical direction, control, and coordination of all information systems support tasks.

2.4.5. <u>Headquarters Marine Corps (HQMC) Functional Managers</u>. The HQMC functional managers are responsible for the proper development, funding, training support and distribution of Class IA and Class IC systems.

a. System Documentation. Each Class IA and Class IC AIS is operated in accordance with procedures established by the HQMC functional manager. The most important procedural document is the User's Manual. This manual is published in accordance with IRM-5231-07 and describes the detailed procedures by which the AIS operates.

b. System Training. Training programs are developed by the appropriate functional manager for personnel and users who are directly involved in the AIS operations. Training may be conducted at the local level or as part of a Marine Corps formal school curriculum for a specific AIS.

2.4.6. Local Functional Sponsor. Local functional sponsors such as the Manpower Information Systems Support Officer (MISSO), MIMMS Information Systems Coordination Office (MISCO), and SASSY Management Unit (SMU) are responsible for providing support and guidance for operational matters within their respective areas. The local functional sponsor is the liaison for operational matters between the command and external agencies. They are responsible for local distribution of their respective Class IA, Class IC, and Class IIB software. They are also the on the scene "eyes and ears" for the headquarters functional managers.

2.4.7. Commanding Generals. The Commanding Generals, Marine Forces, Atlantic; Marine Forces, Pacific; and the Marine Reserve Force publish standard operating procedures to subordinate commanders as required to manage the FMF-EUCE Program.

2.4.8. Regional Automated Services Center (RASC). The RASC is responsible for accepting and processing Class IA data and data aggregation as required.

2.4.9. Marine Corps Central Design Activity (MCCDA). The MCCDA's are tasked by functional managers for the development, maintenance and modification of the Class IA and Class IC applications.

2.4.10. FMF-EUCE Contractor. The contractor is responsible for providing FMF-EUCE hardware and software, and for maintaining such items in accordance with the provisions of the contract.

2.4.11. Marine Corps Systems Command. The Marine Corps Systems Command is responsible for managing and enforcing the provisions of the FMF-EUCE contract, providing sufficient provisioning for the FMF-EUCE, and modifying the FMF-EUCE program as users' needs are changed and new requirements are validated by CG, MCCDC.

2.4.12. Marine Corps Combat Development Command (MCCDC). CG, MCCDC is responsible for two functions:

a. <u>Deputy Commander for War Fighting (Code WF-11A)</u>. The Warfighting Center is responsible for determining and validating FMF requirements.

b. <u>Deputy Commander for Training and Education (Code TE-24)</u>. Computer Sciences School (CSS) is responsible for providing FMF-EUCE training to the Marine Corps data processing personnel in Occupational Field 40.

2.4.13. <u>Assistant Chief of Staff, Command, Control, Communications, Computer, and Intelligence (C4I)</u>. The AC/S C4I is responsible for two functions:

a. The AC/S C4I is responsible for centralized policy formulation, technical direction, acquisition, and interoperability as it relates to AISs and their functioning on the FMF-EUCE.

b. <u>The Marine Corps Computer and Telecommunications Activity (Code MCCTA)</u>. Acting under the direct cognizance of C4I, MCCTA is responsible for the FMF-EUCE capacity management program. MCCTA executes the responsibility through their oversight mission of AIS development, periodic inventories, and enforcement of Life Cycle Management regulations.

2.5. <u>FUNCTIONAL RELATIONSHIPS</u>

2.5.1. <u>Supply Support</u>. Supply support is provided through normal supply channels.

2.5.2. <u>Budget Support</u>. Budget guidance will be provided annually in the Field Budget Guidance (Marine Corps Bulletin 7100 series) prepared by the Deputy Chief of Staff for Installations and Logistics (DC/S I&L). Specific input for ADP budgets is supplied by the CMC (Code CC), as mandated by Congress. HQMC will budget for original procurement of FMF-EUCE. Budgeting for maintenance, consumables, and replacement equipment is the responsibility of the owning unit.

2.5.3. <u>Hardware Maintenance</u>. Maintenance is included as a feature of the FMF-EUCE contract and, as such, is the responsibility of the contractor. Contract administration is the responsibility of the Marine Corps Systems Command. The maintenance concept will be based on numbers of devices procured and cost-effectiveness of user versus contractor maintenance. Current maintenance policy is spelled out in the Material Fielding Plan (MFP).

2.5.4. <u>Software</u>. The software associated with the equipment consists of systems software and application software (Class IA, Class IC, and Class IIB).

a. <u>Systems Software</u>. This software, consisting of the operating system, system utilities, and vendor-provided applications packages, is provided and maintained by the contractor. The contractor retains responsibility for the maintenance of this software for the full service life of FMF-EUCE. Note that prior to any field activity upgrade of the Disk Operating System (DOS) on a Zenith Z-248 or FMF-EUCE utilized for Class IA processing, the Class IA System in question would have to be tested by the appropriate MCCDA for compatibility under the new version of DOS.

b. <u>Class I (A and C) Application Software</u>. By definition, these applications execute on the FMF-EUCE, have Marine Corps-wide applicability, and are sponsored by Headquarters Marine Corps functional managers. Accordingly, all requests for maintenance or modification associated with these applications will be forwarded through the appropriate chain of command to the appropriate Headquarters functional manager in accordance with the current edition of MCO P5231.1.

c. <u>Class IIB Application Software</u>. These applications are developed to meet local commanders' needs. The only formal development requirements for these applications are that they be documented in accordance with IRM-5231-07 (User's Manual) and IRM-5231-08 (Computer Operations Manual), both of which are published under the authority of MCO 5271.1. An inventory of Class IIB application software is published annually in Annex II of the Mid-Range Information Systems Plan.

CLASS IA AND CLASS IC SOFTWARE

(This page intentionally left blank)

Chapter 3

CLASS IA AND CLASS IC SOFTWARE

3.1. CLASS IA AND CLASS IC IMPLEMENTATION. Initial implementation of Class IA and Class IC systems will be conducted based on functional manager guidance.

3.1.1. Notification. Functional managers will notify the implementation site of an impending Class IA and Class IC implementation by Naval Message at least 45 days in advance of the scheduled implementation. The message addressees will include the command ISMO, local RASC, sponsoring MCCDA, and local functional representatives. The purpose of the notification is to ensure availability of hardware and personnel.

3.1.2. Implementation Plan. The functional manager will distribute an implementation plan, that adheres to the format and content of IRM-5231-16 (Implementation Plan), to the same addressees as the notification message no later than 30 days prior to the scheduled Class IA implementation.

3.2. CLASS IA AND CLASS IC DISTRIBUTION. Distribution of Class IA and IC AIS's to users will be coordinated between the functional manager and the system sponsor. The functional manager will notify the MCCDA system sponsor of any changes to the distribution list.

3.2.1. Notification of Receipt. Upon receipt of all releases, recipients will report receipt by Letter of Transmittal or Naval Message to the sending system sponsor.

3.2.2. Contents of New Releases. At a minimum, new releases will contain:

    Revised application software,
    Effective date of implementation,
    Revised User-Operator Manual (UOM) (on floppy diskette, if feasible),
    Summary of all changes,
    Instructions for units participating in extended deployments,
    A point of contact for further information.

3.2.3. Data Aggregation and Message Editing and Processing System (MEPS) Distribution. Distribution of Data Aggregation and MEPS software will be the same as above except that the Director of IRMD Albany will be added to the list.

3.3. MEDIA LABELING STANDARDS. External diskette labels will comply with figures 3-01 and 3-02. (Labels packaged with the

diskettes are acceptable and can be printed using 17 pitch mode).
External tape labels will comply with figure 3-03.

```
1._____2._____
3._____
4._____
5._____
6._____
```

1. Application Area (e.g., MIMMS, AV3M, etc.).
   Include complete release number.
2. Owning Unit.
3. Program/System Description/File Name (if diskette
   contains more than one dataset, enclose a sector/
   header listing in diskette envelope).
4. Special instructions.
5. Point of contact in case of problems.
6. Functional manager unique data.

Example:

```
1._UCTS 1-88_____2._1st Bn,1st Mar,1stMARDIV_
3._Unit Commander's Training System_____
4._Place in slot 1 of diskette drive and press enter_
5._Lt Joe MARINE 555-2222_____
6._____
```

FIGURE 3-01
FMF-EUCE Diskette Labeling (Applications)

```
1._____2._____
3._____
4._____
5._____
6._____
```

1. Application Area (e.g., MIMMS, AV3M, etc.).
    Include complete release number.
2. Owning Unit.
3. Program to which data will be input.
4. Julian Date, Diary Number, or other identification
    of a specific batch of input. All except the
    current entry should be lined out with a felt-tip
    pen.
5. Point of contact in case of problems.
6. Functional manager unique data.

FIGURE 3-02
FMF-EUCE Diskette Labeling (Data)

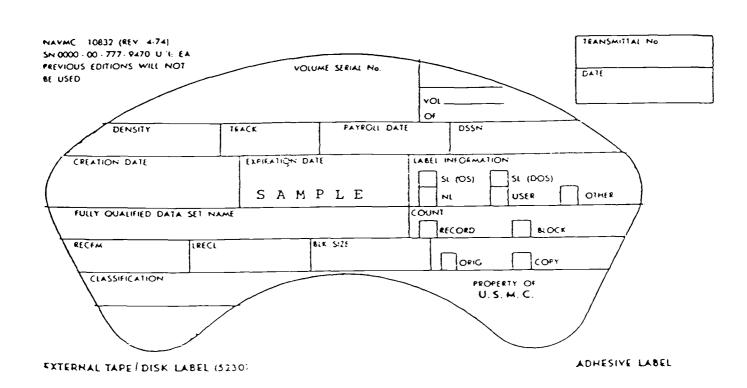
FIGURE 3-03
External Tape/Disk Label

3.4. <u>SOFTWARE STANDARDS</u>. All software will be written in the programming language Ada and in conformance with IRM-5234-02 (Man-Machine Dialogue) and IRM-5234-01 (Programming Standards). Requests for waivers from the use of Ada must be submitted to the Commander, Naval Information Systems Management Center (NISMC) via Director, MCCTA. The waiver format is provided in appendix F.

3.5. <u>FUNCTION KEYS</u>. Function keys will be defined as in IRM-5234-02, Chapter 2, paragraph 2.1.1.b, and labeled accordingly.

3.6. <u>USE OF COLOR</u>. Because of the number of non-color monitors in the inventory, software will not require the user to have a color monitor.

3.7. <u>USE OF RAM</u>. Developers must recognize that approximately half of the inventory are LAN-connected. Therefore, applications must be designed knowing that the resident terminal network operating system uses much of the PC's resident random access memory (RAM).

3.8. <u>MODIFICATIONS</u>. Requests for modifications to Class IA or IC software, requests for new Class IC software, and requests to make an existing Class IIC into a Class IC must be handled in accordance with the current version of MCO P5231.1, Life Cycle Management for Information Systems (LCM-IS).

SECURITY STANDARDS FOR FMF-EUCE

(This page intentionally left blank)

4.3. HARDWARE SECURITY

4.3.1. General. An FMF-EUCE device which processes classified and/or unclassified sensitive information is subject to computer security procedures and formal system accreditation as outlined in this chapter. Unclassified sensitive information is defined to be sensitive by law, regulation, or by the data's originator (e.g., data subject to the Computer Security Act of 1987, the Privacy Act of 1974, Financial Integrity Act of 1982, and National Security interests that relate to the national defense or the foreign relations of the U.S. Government). Sensitive information is information which requires protection from unauthorized access.

4.3.2. TEMPEST Standards. Prior to use in processing classified information, all peripheral equipment to be connected to the FMF-EUCE will meet the standards of one of the following TEMPEST categories:

   a. TEMPEST Certified. FMF-EUCE is considered TEMPEST certified if it passes an Instrumented TEMPEST Survey. This Survey will be performed by the vendor prior to equipment fielding.

   b. TEMPEST Accredited. FMF-EUCE must be TEMPEST accredited. Marine Corps Systems Command will ensure that the FMF-EUCE meets the appropriate security requirements of the National Security Subcommittee on Compromising Emanations National Tempest Standards (NACSEM No. 5100 or NACSIM No. 5100A, "Compromising Emanations Laboratory Test Standard Electromagnetic (U)").

   c. TEMPEST Approved. FMF-EUCE in this category may or may not be TEMPEST certified or TEMPEST accredited. FMF-EUCE meets TEMPEST approval standards as a result of its positioning within a controlled space and the volume and level of classified information processed on the FMF-EUCE. The Naval Security Group (NavSecGru) grants this approval based upon a TEMPEST Vulnerability Assessment Request (TVAR).

4.3.3. TEMPEST Vulnerability Assessment Request (TVAR). A TVAR shall be submitted to the Naval Security Group in accordance with OPNAVINST C5510.93 before an FMF-EUCE device may process classified information (Within CONUS a TVAR is needed for processing secret and above). Upon submission of this written request the system has interim approval to process classified material. Appendix G provides details from the current version of OPNAVINST C5510.93 on the required documentation for a TVAR. A completed TVAR is considered classified information and should be treated as such. OPNAVINST C5510.93 is available through the command Classified Material Control Center (CMCC).

4.3.4. Field Use/Tactical Environments. FMF-EUCE is·considered a transportable "Classified Information Processing (CLIP)

System." Controlled Space (CS) requirements for such a system
are a minimum of 50 meters unless an instrumented TEMPEST survey
or test shows the need for a larger CS. In the case of the FMF-
EUCE, the device meets NACSIM 5100A specifications at a distance
of one meter. Therefore, users can rely on a significantly
smaller CS. The initial TVAR submission should include the
location of the CLIP when deployed, showing the minimum distance
in meters, from CLIP components to the boundary of the CS. This
will eliminate the need to submit a new TVAR whenever an FMF-EUCE
device is moved to the field.

4.3.5. Classification Level. FMF-EUCE users shall possess the
proper security clearance for the highest classification of data
accessible through the system and possess the need-to-know for
all of the information accessible through the system. Each
component of the system will be powered on and off before
processing a different level of classification, such as changing
from a system high of Secret to a system high of Confidential.

4.3.6. TEMPEST Integrity. The FMF-EUCE is restored to its
TEMPEST condition if the approved maintenance procedures are
followed while adding and replacing cards. The Material Fielding
Plan (MFP) contains specific guidance on maintenance procedures
for the FMF-EUCE. The FMF-EUCE loses its TEMPEST integrity if
third party cards (other than those offered on the AN/UYK
contract or AN/UYK spare parts contract) are installed. In
addition, some peripherals may be externally attached to the FMF-
EUCE without violating the TEMPEST integrity of the EUCE device.
Non-TEMPEST equipment (such as LAN cabling) may be attached to
the FMF-EUCE while the device is processing unclassified data.

4.4. SOFTWARE SECURITY

4.4.1. Floppy Diskettes. All floppy diskettes will be color
coded according to the highest classification of their
information. The diskette jacket (the Mylar plastic envelope
which surrounds the magnetic medium) will be colored in its
entirety, according to the following color codes as depicted in
Director of Central Intelligence Directive (DCID) 3/14:

   a. Unclassified - Black, White and Gray.

   b. Unclassified Sensitive (financial, social security
numbers, etc.) - Green.

   c. Confidential - Blue.

   d. Secret - Red.

   e. Top Secret - Orange.

   f. Sensitive Compartmented Information (SCI) - Yellow.

4.4.2. <u>Classified Diskette Ordering Procedures</u>. A request for purchase of color coded diskettes (for classified processing) may be placed through normal open purchase procedures. The diskettes will come from the manufacturer in heat shrunk packages. When the heat seal has been broken, all of the diskettes in the package will immediately become accountable and will be afforded the protection required for a document of the classification indicated by the color of the diskette. This policy is in effect regardless of whether or not the diskette contains information. Refer to IRM-5239-08, "Computer Security Procedures," Appendix C, for ordering information for color coded diskettes.

4.4.3. <u>Classified Diskette Handling Procedures</u>. Diskettes marked SCI, when assigned an SCI control number will be controlled and accounted for by the Special Security Officer (SSO) in accordance with DoD C-5105.21-M-1. Top Secret diskettes will be controlled, handled, and accounted for in accordance with OPNAVINST 5510.1. All other classifications will be handled in accordance with OPNAVINST 5510.1 and local procedures. Control numbers, dissemination control information (e.g., restricted and Not Releasable to Foreign Nationals (NOFORN)), and the owning organization will be written on non-SCI diskette jackets using an indelible ink marker. Ballpoint pens will not be used because they may damage the diskette. SCI diskettes will be marked in the same fashion except they will be also marked with the appropriate compartments and codewords. Unclassified system diskettes and other unclassified diskettes containing executable programs will be write-protected before they are inserted into a system which is processing classified information.

4.4.4. <u>Downgrading/Disposal of Diskettes</u>. Diskettes will not be downgraded, upgraded or declassified with the exception of those containing SCI material. SCI material will be handled in accordance with Defense Intelligence Agency Manual (DIAM) 50-4. The primary means of diskette destruction is incineration. Those commands who are not permitted or do not have the facilities for incineration are authorized to use an alternative method of diskette destruction, as outlined in CSC-STD-005-85 (DoD Magnetic Remanence Security Guideline): degauss the diskette using NSA approved degausser or shred the diskette using a shredder authorized for classified information. The shredded pieces may be disposed of as unclassified waste. If the diskette cannot be shredded as a unit, remove the magnetic media from the colored envelope and shred the magnetic media. Destruction of media containing SCI material will be conducted in accordance with DoD C-5105.21-M.1 and the Navy Supplement to DoD C-5105.21-M.1. Diskettes received from vendors and sources outside the Marine Corps which are not color coded appropriately will be copied onto a properly colored diskette before its use, if authorized or feasible. In cases where copyright law or copy protection prohibits copying vendor software, the diskettes will be labeled with a color coded label as previously described in paragraph 4.4.1. This allowance applies to <u>ONLY</u> vendor provided software.

4.4.5. Other Media. All other removable magnetic media (such as removable hard disk drives, magnetic tapes or paper tape punches) which contain classified data will be accounted for by the highest classification of data that they have ever contained in accordance with OPNAVINST 5510.1 (non-SCI), DoD C-5105.21-M-1 (SCI), and local procedures. Media will be declassified or destroyed in accordance with CSC-STD-005-85. Media will be labeled with a color coded sticker as previously described in paragraph 4.4.1. All color coded labels are available through normal Marine Corps supply channels (stock numbers are provided in paragraph 4.6.4.). Furthermore, a data descriptor label will be affixed to the media indicating the classification, control number, dissemination control information (e.g., restricted and NOFORN), and the owning organization. Use compartments/ codewords, telephone numbers, content, and comments, where applicable.

4.5. DATA SECURITY

4.5.1. General. The objectives of data security for the FMF-EUCE Program are to preserve and protect the integrity of all data bases associated with FMF-EUCE, and to assure that all such data bases receive appropriate protection from unauthorized access, use, or modification. Specific safeguards must be tailored to the existing circumstances with consideration given to sensitivity of the data, continuity of operations, general security of the area, and the cost of safeguards.

4.5.2. Procedures for Data Security

    a. Access Control. Restriction on physical access to data, whether in raw or processed (data base) form, is fundamental to proper data security.

    b. Manpower Data Bases. In addition to the above requirements, local manpower data bases must be considered to be information protected as required by the Privacy Act of 1974.

    c. Consolidation of Dissimilar Data Bases. In many circumstances, the contents of a data base may be unclassified. However, when combined with another unclassified data base (such as MIMMS information combined with certain SASSY information), THE RESULTING DATA BASE MAY BE CONSIDERED SENSITIVE OR CLASSIFIED.

    d. Processing of Classified Information on the Hard Disk Drive. An FMF-EUCE Removable Hard Disk Drive which is used to process Class IA Automated Information Systems (AIS's) should not be used to process classified information. If a Hard Disk Drive is used to process classified information, then the hard disk drive would have to be considered classified, and could no longer be used for unclassified AIS's. The preferred method for storing

classified data, is to store the data onto color coded floppy
disks.

4.6. ACCREDITATION

4.6.1. System Accreditation Process Overview. System
accreditation (as opposed to being TEMPEST accredited) is a
formal statement by a designated approving authority (DAA)
stating that all known vulnerabilities and risks associated with
a computer-based system have been considered, and all cost
effective countermeasures have been implemented, tested, and
found to be effective. Countermeasures to consider include the
areas relating to administrative, procedural,
physical/environmental, personnel, communications security
(COMSEC), and computer-based controls (i.e., hardware and
software). FMF-EUCE systems and all networks to which they are
connected are to be accredited to the maximum specified level of
sensitivity (Unclassified Sensitive, Confidential, Secret, Top
Secret, or SCI). All systems which will be used to process or
access classified information (secret or higher in CONUS) must
have had a TVAR (see Appendix G) submitted before they can be
system accredited. Systems must be re-accredited at least every
three years or whenever the system is re-configured in a way
which significantly changes the risks and vulnerabilities
associated with it.

4.6.2. System Accreditation Authority. All Marine Corps
organizations operating FMF-EUCE devices will accredit them
before the machines are used to process or store classified or
unclassified sensitive information. Designated Approval
Authorities (DAAs) for FMF-EUCE are listed in paragraph 11005 of
MCO 5510.14, the Marine Corps ADP Security Manual.

4.6.3. System Accreditation/Labels. System accreditation will
not become effective until a formal, dated, statement of
accreditation has been issued by the DAA as a result of a system
accreditation review addressed in paragraph 4.5.2. above. The
statement of system accreditation will include the specified
level of sensitivity or classification for which the
accreditation has been granted, a statement by the DAA as to the
acceptability of identified risks (where applicable), and any
exceptional circumstances incumbent to system accreditation.
This brief statement should be adequate for purposes of
subsequent system accreditation reviews and system
re-accreditation. When an FMF-EUCE standard configuration
(system unit, monitor, keyboard, and printer), or peripheral
devices cabled to the system unit, have been formally accredited,
or have received the DAA's interim authority to process
classified information (to include a formal TVAR), a system
accreditation label (sticker) that specifies the highest level of
system sensitivity will be placed on each device in a conspicuous
place. The rectangular block on the label will reference the
DAA's accreditation or interim authority to operate. System

accreditation labels are available through normal Marine Corps supply channels.

4.6.4. Label Requisitioning. Listed below are the stock numbers for ordering magnetic media classification labels and systems accreditation labels through normal Marine Corps supply channels.

    a. Magnetic Media Classification Labels:

        (1) Sensitive Unclassified, NAVMC 11196, Stock No. 0000-00-007-0100, PAD=50.
        (2) Confidential, SF 708, NSN 7540-01-207-5538, PAD=300.
        (3) Secret, SF 707, NSN 7540-01-207-5537, PAD=300.
        (4) Top Secret, SF 706, NSN 7540-01-207-5536, PAD=300.
        (5) Data Descriptor, SF 711, NSN 7540-01-207-5541, PAD=300.
        (6) SCI, NAVMC 11179, Stock No. 0000-00-006-9680, PAD=50.

    b. System Accreditation Labels:

        (1) Sensitive Unclassified, NAVMC 11180, Stock No. 0000-00-006-9700, PAD=50.
        (2) Confidential, NAVMC 11181, Stock No. 0000-00-006-9720, PAD=50.
        (3) Secret, NAVMC 11182, Stock No. 0000-00-006-9740, PAD=50.
        (4) Top Secret, NAVMC 11183, Stock No. 0000-00-006-9760, PAD=50.
        (5) SCI, NAVMC 11184, Stock No. 0000-00-006-9780, PAD=50.

4.7. REFERENCES. Most of the directives listed below are referenced in this chapter and serve as the authority for implementing the controls, procedures, and requirements contained herein. These documents are normally available through the CMCC.

    DoD C-5105.21-M-1, "SCI Security Manual-Administrative Security"

    Navy Supplement to DoD C-5105.21-M-1, "SCI Security Manual-Administrative Security"

    DoDD 5200.28, "Security Requirements for Automated Information Systems (AIS)"

    DIAM 50-4 (C), "Security of Compartmented Computer Operations"

    DCID 3/14, "Standards for Security Labeling of Removable ADP Storage Media"

OPNAVINST C5510.93, "DON Implementation of National Policy on Control of Compromising Emanations"

OPNAVINST 5510.1 "DON Information Security Program Regulation"

OPNAVINST 5239.1, "DON ADP Security Program"

SECNAVINST 5239.2, "DON AIS Security Program"

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

MCO P5271.1, "IRM Standards and Guidelines Program" (Technical Publications)

IRM-5239-08, "Computer Security Procedures"

CSC-STD-005-85, "DoD Magnetic Resonance Security Guideline"

FMF-EUCE AIS GUIDELINES
IRM-5230-01A

Chapter Table of Contents

Chapter 5

DATA COMMUNICATIONS

(This page intentionally left blank)

Chapter 5

DATA COMMUNICATIONS

5.1. <u>COMMUNICATIONS OVERVIEW</u>. A major feature of the FMF-EUCE device is its capability to communicate with other computers. The internal modem is capable of providing asynchronous communications via the COM1 port which is a component of every designated system. Additionally, the asynchronous communications capability can be replaced with a synchronous data link control (SDLC) capability in order to transmit data to the mainframe computers at Remote Job Entry (RJE) facilities, Regional Automated Services Centers (RASC's), Deployable Force Automated Services Centers (DFASC's), and Marine Corps Central Design Activities (MCCDA's) through a compatible communications controller.

5.2. <u>ASYNCHRONOUS COMMUNICATIONS</u>. Asynchronous communications can be defined as a scheme for transmitting data where each character is preceded by a start bit and followed by a stop bit, thus permitting data elements to occur at irregular intervals. Asynchronous data communications have been performed on many types of communication mediums in the Marine Corps inventory. Virtually any of the transceiver type communication equipment can be used, as long as it is capable of constant keying. Additionally, transmissions should be encrypted by either software or hardware methods whenever possible. Only encryption hardware/software that has been approved by the National Security Agency (NSA) will be used. For detailed information on equipment identification, step-by-step setup procedures and troubleshooting involved with asynchronous data communications, refer questions to the local ISMO.

5.2.1. <u>Transmitting Data</u>. Using asynchronous data communications software provided with the FMF-EUCE system, a user can transmit data at a rate of between 300 to 2400 bits per second using the following methods:

   a.   FMF-EUCE to FMF-EUCE using WD-1/PTT (slash wire).

   b.   FMF-EUCE to FMF-EUCE using telephone switchboards.

   c.   FMF-EUCE to FMF-EUCE using local area networks.

   d.   FMF-EUCE to FMF-EUCE using high frequency communications.

   e.   FMF-EUCE to FMF-EUCE using very high frequency communications.

   f.   FMF-EUCE to FMF-EUCE using ultra high frequency communications.

g. FMF-EUCE to FMF-EUCE using super high frequency communications.

5.2.2. WD-1/PTT. WD-1/PTT or slashwire is a common, available medium for data communications connections between FMF-EUCE devices.

5.2.3. Switchboard. The tactical switchboards, SB-3082, SB-3614 or the future AN/TTC-42 (Unit Level Circuit Switch) can all be used to establish a local area network using the switchboard as a Private Branch Exchange (PBX). Only the SB-3082 requires intervention by the switchboard operator to manually connect two FMF-EUCE devices prior to passing data traffic; the others operate automatically.

5.2.4. Local Area Network (LAN). LAN's enable the connection of more than two FMF-EUCE devices to pass data traffic simultaneously, which is the limitation of the tactical switchboard above. IRM-5239-04, Local and Wide Area Networks, contains standards to be used in acquiring any LAN product. It should also be noted that internal and external LAN hardware will interfere with the TEMPEST integrity of the AN/UYK-83, affect the warranty and maintenance procedures, and invalidate the TEMPEST certification.

5.2.5. High Frequency (HF). HF radios enable long range, over-the-horizon communications capability. The FMF-EUCE can be connected to this communications equipment to transmit data over long distances from the Amphibious Objective Area (AOA) to rear echelons for bulk processing. Examples of HF communication equipment are the AN/MRC-138, AN/GRC-193 and AN/TSC-95.

5.2.6. Very High Frequency (VHF). VHF radios enable medium range (15-20 miles), line-of-sight communications capability. The FMF-EUCE device can be connected to this communications equipment to transmit data over medium distances within the AOA to transmit time-sensitive or tactical reports from one unit to another for local processing. Examples of VHF communication equipment are the AN/PRC-77 and RT-524. Additionally, VHF multichannel equipment (e.g., AN/TRC-166 and AN/MRC-135) allows up to eight separate communications channels for simultaneous data transmission, if available.

5.2.7. Ultra High Frequency (UHF). UHF radios enable short to medium range (5-20 miles), line-of-sight communications capability. The FMF-EUCE device can be connected to this communications equipment to transmit time-sensitive and tactical reports over short to medium distances within the AOA from one unit to another for local processing. Examples of UHF communication equipment are the AN/PSC-3 and the future AN/TSC-96.

5.2.8. <u>Super High Frequency (SHF)</u>. SHF radios enable short to very long range (0-25,000 miles), around-the-world communications capability. The FMF-EUCE device can be connected to this communications equipment to transmit data any distance from one unit to another for processing. Examples of SHF communication equipment are the AN/GRC-201, AN/TSC-85 and AN/TSC-93. For setup instructions, consult local CEO.

5.3 <u>SYNCHRONOUS DATA LINK CONTROL (SDLC) MAINFRAME COMMUNICATIONS</u>. SDLC is defined as the transmission in which data characters and bits are transmitted at a fixed rate with the transmitter and receiver synchronized. Using SDLC communications, the FMF-EUCE device can be used as a remote job entry device for transmission of data directly to and from mainframe computers. SDLC 3278/9 terminal emulation consists of emulation software/firmware and user documentation. Two separate means of communication are provided:

    a. 3278/9 Emulation Via Coaxial Connection.

    b. 3278/9 Emulation Via RS-232-C Connection.

5.3.1. <u>3278 Emulation Via Coaxial Connection</u>. Using IBM 3278/9 terminal emulation software/firmware, a coaxial connection is established to an "A" port of an IBM 3274 series, IBM 3276 series, or compatible control unit via coaxial cable. The control unit is attached either locally or via an SDLC modem to a communications controller and further into the mainframe. A file transfer function between the FMF-EUCE and a host mainframe executing the MVS/TSO 3270-PC File Transfer Program, IBM Program Number 5665-311 is provided.

5.3.2. <u>3278 Emulation Via RS-232-C Connection</u>. Emulating a 3274 cluster control unit, the interface communicates via synchronous modem through a communications controller to the mainframe computer. The 3278/9 terminal emulation and 3287 printer emulation is provided. A file transfer function between the FMF-EUCE and a host mainframe executing the MVS/TSO 3270-PC File Transfer Program, IBM Program Number 5665-311 is also provided.

5.3.3. <u>3770 RJE Workstation Emulation</u>. Emulating a 3770 RJE workstation, the interface communicates via synchronous modem through a communications controller to the mainframe computer. The interface provides the functions of IBM 3770 console, reader, punch, printer, and diskette RJE input and output functions using the SNA Character Stream (SCS) data stream.

(This page intentionally left blank)

Appendix A

GLOSSARY OF TERMS AND ABBREVIATIONS

Ada   The standard programming language for FMF-EUCE

ADP   Automatic Data Processing

ADPE-FMF   Automatic Data Processing Equipment for the Fleet
                    Marine Force

AIS   Automated Information System

Asynchronous   A scheme for transmitting data where each
                    character is preceded by a start bit and followed
                    by a stop bit, thus permitting data elements to
                    occur at irregular intervals.

ATRIMS   Aviation Training Readiness Information
                    Management System

AUTODIN   Automatic Digital Network

AUTOVON   Automatic Voice Network

BSSG   Brigade Service Support Group

Byte   A sequence of 8 adjacent binary digits operated
                    on as a unit by the computer.

CCT   Telecommunications Branch of C4 Division

CEO   Communications-Electronics Officer

Class I   An AIS for which the AC/S C4I provides development
                    guidance, that operates on a mainframe computer,
                    is sponsored by a HQMC functional manager, and
                    serves Marine Corps-wide users.

Class IA   A Class I derivative which supports the data input
                    and output functions of a parent Class I system
                    (i.e., a Class IA acts as a feeder system to a
                    Class I mainframe or mini system). This Class IA
                    is processed on mini or microcomputers organic to
                    the SE and/or the FMF and supports Marine
                    Corps-wide users.

Class IC   A Class I system that is processed on
                    microcomputers organic to the SE and/or FMF and
                    supports Marine Corps-wide users. Class IC
                    systems have no parent mainframe application.

Class II	An AIS that operates on a mainframe computer and supports the local needs of a HQMC staff agency, an FMF unit, or a SE organization.
Class IIB	An AIS that operates on a microcomputer and supports the local needs of a HQMC staff agency, an FMF command, or a SE organization.
CLIP	Classified Information Processing
CMC	Commandant of the Marine Corps
COMNAVINTCOM	Commander Naval Intelligence Command
COMNAVSECGRU	Commander Naval Security Group
COMSEC	Communications Security
CONUS	Continental United States
CPU	Central Processing Unit
CS	Controlled Space
CSS	Computer Sciences School
CXI's PCOX	3278 Emulation Card
DA	Data Aggregation
DAA	Designated Approving Authority
DAD	Diskette Duplication/Aggregation Device
DAS	Data Aggregation System
DATA AGG	Data Aggregation
DCID	Director of Central Intelligence Directive
DCS	Defense Communications System
DFASC	Deployable Force Automated Services Center
DIAM	Defense Intelligence Agency Manual
DoD	Department of Defense
DOS	Disk Operating System
ELMACO	Electronic Maintenance Company
EMI	Electromagnetic Interference

FASC	Force Automated Services Center
FMF	Fleet Marine Force
FMF-EUCE	Fleet Marine Force - End User Computing Equipment
FSSG	Force Service Support Group
FTS	Federal Telephone System
GSA	General Services Administration
HF	High Frequency
HQMC	Headquarters Marine Corps
ILSP	Integrated Logistics Support Plan
IRM	Information Resources Management
ISMO	Information Systems Management Officer
LAN	Local Area Network
LCM	Life Cycle Management
LCM-IS	Life Cycle Management for Information Systems
MAGTF	Marine Air Ground Task Force
MB	Megabyte
MCCDA	Marine Corps Central Design Activity
MCCDC	Marine Corps Combat Development Command
MCCTA	Marine Corps Computer and Telecommunications Activity
MCO	Marine Corps Order
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
MEPS	Message Editing and Processing System
MFP	Material Fielding Plan
MIMMS	Marine Corps Integrated Maintenance Management System

MNS	Mission Need Statement
MRISP	Mid-Range Information Systems Plan
NAVFLIRS	Naval Flight Record Sub-System
NCS	Naval Communications System
NISMC	Naval Information Systems Management Center
NOFORN	Not Releasable to Foreign Nationals
NSA	National Security Agency
OLDS	On-Line Diary System
PBX	Private Branch Exchange
RASC	Regional Automated Services Center
RJE	Remote Job Entry
SASSY	Supported Activity Supply System
SCI	Sensitive Compartmented Information
SCS	SNA Character Stream
SDLC	Synchronous Data Link Control
SE	Supporting Establishment
SHF	Super High Frequency
SLS	Source Library System
SMU	SASSY Management Unit
SNA	System Network Architecture
SSO	Special Security Officer
Synchronous	Transmission in which the data characters and bits are transmitted at a fixed rate with the transmitter and receiver synchronized.
T/E	Table of Equipment
TEMPEST	Unclassified short name referring to investigations and studies of compromising emanations.
3M	Maintenance Material Management System

TSO	Time Sharing Option
TVAR	TEMPEST Vulnerability Assessment Request
UHF	Ultra High Frequency
UM	User's Manual
UOM	User-Operator Manual
VHF	Very High Frequency
WTI	Weapons Tactical Instruction
Z-248	Zenith Z-248 Microcomputer

(This page intentionally left blank)

Appendix B

CLASS IIB AUTOMATED INFORMATION SYSTEMS

PART I - FMF-EUCE CLASS IIB AUTOMATED INFORMATION SYSTEMS
         DEVELOPMENT PROCESS FOR INFORMATION SYSTEMS MANAGEMENT
         OFFICERS (ISMO'S)

1. GENERAL. The Force Service Support Group (FSSG) ISMO and the
Brigade Service Support Group (BSSG) ISMO is charged with
providing FMF-EUCE Class IIB applications software support to
systems users within his respective MEF or MEB. The setting of
standards for FMF-EUCE Class IIB software development procedures
is required to ensure the uniformity, quality, and
maintainability of all applications developed at the local level.
The standards are structured to assist commanders in the design
of well-formulated, efficient local software applications and to
provide a model from which all FMF-EUCE Class IIB software
applications may be developed.

2. ORGANIZATION FOR APPLICATIONS DEVELOPMENT. The organization
for the development of Class IIB AIS's will depend on the
complexity of the project and upon personnel availability.
Simple requests may be managed by the project manager/systems
analyst and the originator of the request. More complex
requirements may necessitate the formation of a project team.
The project team should include representatives from the unit
organizing the request, the major command level functional
representative, the ISMO, and other technical representatives as
necessary. The managerial group provides assistance and guidance
to the programming team during the development effort. The
programming team should always include a project manager/systems
analyst and a programmer. In addition, it is recommended that
Annex II of the Marine Corps Mid-Range Information Systems Plan
(MRISP) be reviewed prior to developing any Class IIB
applications. This will preclude any duplication of
microcomputer applications which may be used by both base and FMF
units. The project team concept is applied in the following
procedures:

     a. DEVELOPMENT MANAGEMENT PROCEDURES. The paragraphs below
describe the specific phases of LCM to be followed by commanders
in the development of FMF-EUCE Class IIB applications in
accordance with procedures outlined in MCO P5231.1, Life Cycle
Management for Information Systems (LCM-IS) Projects. The
individual requesting FMF-EUCE Class IIB programming support will
usually be the FMF-EUCE user (e.g., battalion/squadron S-1/S-2,
major command G-1, G-2).

          (1) Mission Analysis/Project Initiation. The purposes
of this phase are to identify and validate a mission element
need, determine significant assumptions and constraints on

solutions, and recommend the exploration of alternative functional concepts to satisfy the need. This phase is completed upon approval of the Mission Need Statement (MNS) at milestone 0.

      (2) <u>Concept Development</u>. The purposes of this phase are to identify user requirements, evaluate alternative methods to satisfy those requirements, and to recommend alternatives for further exploration. This phase is completed upon approval of the concept at milestone I.

      (3) <u>Definition and Design</u>. The purposes of this phase are to fully define the functional requirements and to design the technical portion of the AIS. This phase is completed upon approval of the definition and design at milestone II.

      (4) <u>System Development</u>: The purposes of this phase are to develop, integrate, test, and evaluate the ADP system and the total AIS. This phase is completed when the Functional Manager certifies that the AIS satisfies the mission need, and approval to implement the AIS is granted at milestone III.

      (5) <u>Deployment and Operation</u>. The purposes of this phase are to implement, operate, and maintain the AIS during its life cycle. Milestone IV consists of a periodic review to ensure: (a) that the functional requirements are still being satisfied, or (b) that there is a determination of when to terminate or replace the AIS.

    b. <u>Project Team Completion Procedures</u>. During the Deployment and Operation phase (after implementation of the AIS), the project team will determine the appropriate time to disband. At this time the ISMO will assemble all documentation and correspondence concerning the project and produce a complete project file. An ISMO systems analyst and maintenance programmer will be assigned to the system and will be responsible for completing all maintenance and modifications to the system.

PART II - FMF-EUCE CLASS IIB APPLICATION SOFTWARE DEVELOPMENT
MANAGEMENT PROCEDURES FOR LOCAL USERS

1. GENERAL. Specific FMF-EUCE user application development
management procedures are provided in order to ensure the
effective development of local applications by users. The
standard database management systems for FMF-EUCE are Enable or
dBase III Plus.

2. DEVELOPMENT MANAGEMENT PROCEDURES. The following paragraphs
describe the specific procedures to be followed by the individual
unit or major command staff section in the development of Class
IIB application software.

     a. Step 1: Project Feasibility. A determination must be
made as to whether or not sufficient assets exist within the unit
to accomplish the project. If not, assistance should be
requested from local ISMO, RASC or RJE. Such requests are then
processed as described in Part I of this Appendix. If local
assets are sufficient then proceed to Step 2.

     b. Step 2: Project Design and Implementation. After a
determination that the project will be completed using unit
assets, the project will be designed and programmed by the user.
Required documentation, in accordance with IRM-5231-07 (User's
Manual) and IRM-5231-08 (Computer Operations Manual), should be
prepared by the user. These documents will facilitate the use of
the Class IIB application software by other units, thus
minimizing duplication of effort and providing for more effective
staff turnover.

(This page intentionally left blank)

Appendix C

SOURCE LIBRARY SYSTEM
CLASS II SOFTWARE LIBRARY

1. GENERAL. A Marine Corps centralized software and
documentation library for Class II (locally developed)
applications will not be maintained. However, all Class II
Automated Information Systems (AIS's) which support command-wide
functions or AIS's which support more than one FMF unit must be
entered into the Information Systems Inventory as outlined in
IRM-5271-05 (IRM Planning). The Source Library System (SLS)
Catalog, maintained at MCCTA, Quantico, VA, is a system that
pools available Class II computer programs. Its purpose is to
reduce duplication of software development efforts at local
sites, encourage sharing of Class II AIS's among Marine Corps
commands, and to identify locally developed functions which may
be candidates for conversion to Class IA or Class IC
applications. All new Class II systems should be identified in
the annual submission to the USMC Mid-Range Information Systems
Plan (MRISP). The MRISP Annex II Information Resources
Management Systems Catalog contains the Marine Corps Hardware and
Software Inventory. If desired, command Information Systems
Management Officers (ISMO's) may maintain a local library of
Class II software.

2. PARTICIPATION. The SLS Bulletin Board System (BBS) is
intended to assist ISMO staffs in meeting the ADP development
demands of their supported commands. Consequently, the SLS
administrator will typically grant access only to ISMO staffs.
Technical representatives from several companies have agreed to
log onto the SLS on a weekly basis to offer their expertise. The
SLS Catalog can be found on the BBS and is distributed to all
major ADP sites via the Electronic Library and Mail System
(ELMS).

3. DOCUMENTATION REQUIRED. Users are responsible for properly
documenting locally developed applications in accordance with the
IRM-5231-07 (User's Manual) and IRM-5231-08 (Computer Operations
Manual). All documentation should be prepared in electronic
form, using one of the Marine Corps' standard word processing
packages.

(This page intentionally left blank)

Appendix D

DATA AGGREGATION

1. DEFINITIONS:

    a. Data Aggregation (DA) is the collection and combination
of several volumes of data into a single group of data. This may
consist of data from several organizations or from just one. In
the latter case, DA is the conversion from one magnetic media to
another.

    b. The Data Aggregation System (DAS) is the software that
allows for bulk data transfer between the user's environment,
FMF-EUCE device, and the host.

    c. The Diskette Duplication/Aggregation Device (DAD) is a
non-TEMPESTED, non-ruggedized device designed to provide multiple
diskette aggregation services while demanding a minimum of
operator intervention. Typically, performance of duplication or
aggregation services is the function of the CDA, RASC, or RJE.
However, this function may also be performed by the DFASC, MISSO,
MISCO, SMU and sometimes the ISMO. Duplication and/or
aggregation functions may also be performed on the FMF-EUCE
device as an alternative to utilizing it as a processor. The
primary function of the DAD is to duplicate and/or aggregate, and
it can automatically handle a large numbers of diskettes
simultaneously with minimal operator intervention.

2. BACKGROUND: The current method of DA is accomplished at
various levels, including both the ADP user and the functional
manager sites, for the purpose of providing data to Class I
systems. The present equipment includes ADPE-FMF devices and
commercial Series/1 devices. The DAD has been fielded to those
sites where previous duplication or aggregation series were
performed, or where data volume, diskette volume and/or the
number of supported units has dictated the requirement.

3. FMF-EUCE DATA AGGREGATION: The proposed methods of DA are as
follows:

The user will have three methods of passing data to the host:
CXI/PCOX 3270 "SEND and RECEIVE" programs; "RESPOND" 3270/3770
RJE; and magnetic tape (800 or 1600 BPI). The host data set type
will change depending on the mode each user selects for upload.
CXI/PCOX 3270 will use sequential data sets (DISP MOD) and
"RESPOND" will use generation data groups. The host requirements
will not change for download. Further details will be published
at a later date.

(This page intentionally left blank)

Appendix E

MESSAGE EDITING AND PROCESSING SYSTEM

1. <u>APPLICATION NAME</u>: Message Editing and Processing System (MEPS).

2. <u>OBJECTIVE</u>: To facilitate the preparation of pseudo-data messages on the FMF-EUCE from recorded Information Systems transactions and to provide a message composition and editing capability to unit communications centers.

3. <u>SPONSOR</u>: AC/S C4I, (Code MCCTA).

4. <u>DESIGNER/PROGRAMMER</u>: Systems Development Division, MCCTA (Code CTAA), Quantico, VA.

5. <u>USERS</u>: MEPS will be used by embarked units on a daily basis to assist in the transmission of text messages and Class IA data.

6. <u>APPLICATION DESCRIPTION</u>: MEPS is a composition, editing, and reformatting system that provides for the rapid submission of narrative and data traffic from the deployed unit through the Naval Communications System (NCS) and the Defense Communications System (DCS).

7. <u>DATA FLOW</u>: MEPS consists of three parts: a data entry subsystem, a text entry subsystem, and a tape output subsystem.

    a. The data entry subsystem is provided to create data messages and was the original purpose for the development of MEPS. The subsystem supports all Class IA applications that generate only character data transmittable via AUTODIN.

    b. The text subsystem allows a user to create a free form naval message.

    c. The tape output subsystem creates the paper tape or magnetic tape output containing the naval message and is described in detail in the User's Manual (UM).

    d. MEPS uses input data files created by other systems such as NAVFLIRS, 3M, and SASSY. MEPS takes these files as its input and combines the information contained therein with appropriate header information supplied by functional area users and communication personnel to create the desired tape output for the NCS. The functional area input file is returned intact to the user. Additionally, MEPS can produce an output diskette containing the stored message for future use.

8. SOFTWARE DISTRIBUTION: Updates and revisions to the MEPS software will be distributed to the MCCDA's, RASC's, and the FSSG ISMO's.

9. MEPS EXECUTION. A fully capable, MCCDA supported MEPS will be available for the FMF-EUCE only.

Appendix F

Ada WAIVER REQUEST FORMAT

Cover Letter: A waiver request package must include a cover letter (not to exceed one page), signed out by the proper releasing authority in the chain of command, to the approval authority Commander, NISMC. Cover letter should include a focal point (office symbol and phone) and a brief summary of the contents of the package. The details are to be included in the subparagraphs below and may not exceed ten pages in length.

Attachment 1, Executive Summary: This attachment includes a description of the capabilities needed, rationale and justification for not using Ada (to include cost, schedule performance, reuse, portability and risk), a description of the proposed system (hardware, software, firmware) and a justification and rationale for selecting the proposed system.

Attachment 2, System/Project Description: This attachment includes details of the proposed system, to include acquisition and contracting status (to the extent it is pertinent to waiver decision), and description of both host and target hardware, software, and firmware.

Attachment 3, Life Cycle Cost Analysis: This attachment provides a cost and benefit analysis which clearly shows that the proposed solution is more cost effective and beneficial to DON over the project's life than Ada. The analysis must address both the Ada solution and the proposed solution and include software development costs, life cycle maintenance costs, replacement costs, training, portability, reuse, productivity, performance, useability, documentation, interfaces, schedules, and higher authority program direction.

When computing the life cycle cost of an Ada solution, any initial investment in Ada support environments, tools training, etc., must be amortized over all future anticipated Ada projects. In such cases the amortized amount of the total investment should not exceed fifty percent, since the investment would be used for future projects.

Attachment 4, Transition Plan: This attachment describes your future plans for moving to Ada if the waiver is approved. Address all applicable factors, including language features, compilers, environments, bindings, training, education, schedules, personnel, costs and hardware.

Attachment 5, Risk Analysis: This attachment describes risks such as schedule, performance, security and other non-economic issues associated with both the Ada and non-Ada solutions.

Attachment 6, Statement of Maintenance: This attachment (limited to one page) must identify the responsible maintenance activity (in-house or contractor) associated with the software involved with the exception request.

Appendix G

TEMPEST VULNERABILITY ASSESSMENT REQUEST (TVAR) (U)

1. Prior to processing classified data (secret and higher within
CONUS), TEMPEST Vulnerability Assessment Requests shall be
forwarded to COMNAVSECINVCOM with a copy to CO, NAVELEXSECCEN,
CMC (CCT), and other commands as appropriate. The following
lists the required information for a TVAR as indicated in
OPNAVINST C5510.93:

    a. Identification of both the command possessing the
Classified Information Processing Systems (CLIPS) and responsible
for its security, and the command submitting the TVAR. Provide
the NTP-3 short title for both and the name and phone number of
points-of-contact at both.

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

    c. Listing and description of the equipment and systems,
including individual system component nomenclature and model
numbers of stand-alone equipment which will process classified
information. Include statements concerning TEMPEST posture of
system/equipment (i.e., off-the-shelf, built or modified to meet
NACSIM 5100, EZN, etc.). In the case of the AN/UYK-83, all
equipment is TEMPEST accredited (meets NACSEM No. 5100 or NACSIM
No. 5100A) except for CLIN's 0006, 0013 through 0019, and 0021.
Include the total volume of data handled and the period over
which such volume is handled. Volume should be in terms of the
type of processing done (e.g., "messages" for a communication
center, "pages" for a printing facility or "screens" if the
processing is done primarily on video terminals). Additionally,
a breakout, in percentages, of the volume at each classification
level should be made and a listing provided of types of
compartmented data, if any, that are processed. Identify
specific equipment deleted, added or relocated since last
instrument TEMPEST survey (ITS) of this equipment.

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

        (1) Manufacturer of enclosure.

        (2) Date installed.

        (3) Installing activity.

        (4) When was the enclosure last tested for RF
attenuation? _____ Attach a copy of the test report.

(5) Have any penetrations been made to the enclosure since the last RF attenuation test?_____YES_____NO.

(6) Is the RF shielding (e.g., fingerstocking) in good repair?_____YES_____NO.

e. Provide as many drawings as are needed to show clearly:

(1) Outline of the building containing the CLIPS and its surrounding outside area, including roadways, loading zones, parking lots, etc.

(2) If applicable, areas outside the building which are protected with alarm systems or which are under continuous surveillance by personnel with at least a U.S. SECRET clearance.

(3) The room numbers and the boundaries of the classified processing and/or compartmented area(s) and the boundaries of the CS's if they differ from the boundaries of the areas.

(4) The classification level of the areas surrounding, above, and below the CS.

(5) Areas within the facility where personnel with less than a U.S. SECRET clearance can obtain access without being properly escorted or under continuous surveillance.

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

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

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

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

i. Will signal lines carrying un-encrypted classified/ compartmented information be routed into areas of lower classification/compartmentalization or into uncontrolled areas?

If so, describe TEMPEST and physical security protective measures. Will compartmented data be transmitted outside the compartmented area? If so, identify organization, location, building, and room number of distant end for each circuit.

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

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

    l. For compartmented processors, are telephone lines:

        (1) Shielded? _____YES _____NO.

        (2) In conduit? _____YES _____NO.

        (3) Filtered? _____YES _____NO. If Yes, are filters grounded within the controlled space? _____YES _____NO.

        (4) Distributed separately from all classified signal lines? _____YES _____NO.

        (5) A minimum of one meter from the CLIPS? _____YES _____NO.

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

(This page intentionally left blank)

COMMENTS/REVISIONS

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

IRM Tech Pub
Name: _____

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

COMMENTS/RECOMMENDATIONS:

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

Name/Rank:
_____ (optional)

Unit:
_____ (optional)

Mail To: United States Marine Corps
           Director CTAS
           MARCORCOMTELACT
           3255 Myers Ave
           Quantico VA   22134-5048

           ELMS - GICISP:MQGMCCTA