

UNITED STATES MARINE CORPS

I MARINE EXPEDITIONARY FORCE, FMF
CAMP PENDLETON, CALIFORNIA 92055-5400

I MEFO P5230.10

G-6 /WWMCCS

27 Apr 1992

I MARINE EXEPDITIONARY FORCE ORDER P5230.10

From: Commanding General

To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE WORLD WIDE MILITARY
COMMAND AND CONTROL SYSTEM AUTOMATED DATA PROCESSING
REMOTE TERMINAL AREA (SHORT TITLE: WWMCCS ADP SOP)

Ref: (a) JCS Pub 22 (WASS Manual)
(b) OPNAVINST 5510.1H (Information and Personnel Security
Program Regulation)
(c) MCO P5510.14 (ADP Security)
(d) JCS Pub 6-03.7 (WIN Security)
(e) IMEFO 5510.5
(f) The Pacific Command WWMCCS Regional ADP Center
(PACWRAC) User's Guide
(g) JDS Retrieval Guide
(h) JDS Procedures Manual
(i) JDS User's Manuals
(j) JOPEs Volume I (General Reference User's Manual)
(k) JOPS User's Manuals
(l) JDSSC, TM 245-88 (WMCCS Terminal User's Guide)
(m) HQ USEUCOM User's Manual for Enhanced Terminal
Capability (ETC) Version 5.5.0 of 14 May 1991
(n) CMC Washington DC MCOPSLOG TLCF msg #41
(o) AF Manual 50-752 (CDTS User's Manual)

Encl: (1) Locator Sheet

1. Purpose. To establish a standing operating procedure (SOP) for the use and operation of the I Marine Expeditionary Force (MEF) World Wide Military Command and Control System (WWMCCS) Automated Data Processing (ADP) Remote Terminal Area (RTA).

2. Background. References (a) through (d) provide guidance for the implementation of the JCS WWMCCS, ADP and Department of the Navy Information and Personnel Security Programs. References (e) and (f) provide guidance for the implementation of local WWMCCS and ADP procedures and security programs. References (g) through (l) contain information and procedures for utilizing the Joint Operations Planning and Execution System (JOPEs). References (m) and (n) contain information and procedures for operating within the subsystems of the WWMCCS Intercomputer Network (WIN). Reference (o) provides guidance for


I MEFO P5230.10
27 Apr 1992

students using the Computer Directed Training System (CDTS)
resident in the WIN.

3. Action. The procedures in this Manual are effective upon receipt.

4. Recommendations. Recommendations concerning the contents of WWMCCS ADP SOP are invited. Forward the recommendations to the Assistant Chief of Staff, G-6, Headquarters and Service Company, I Marine Expeditionary Force, MCB Camp Pendleton, California 92055.

5. Certification. Reviewed and approved this date.



B. C. STEED
Chief of Staff

DISTRIBUTION: LIST I/LIST II

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURES FOR THE WORLD WIDE MILITARY
COMMAND AND CONTROL SYSTEM AUTOMATED DATA PROCESSING REMOTE
TERMINAL AREA (SHORT TITLE: WWMCCS ADP SOP)

Location:

(Indicate the location(s) of the copy(ies) of this
Manual)

WWMCCS ADP SOP

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporating Change
------------------	-------------------	-----------------	---

TABLE OF CONTENTS

CHAPTER

1 AREAS	INTRODUCTION TO THE WWMCCS ADP REMOTE TERMINAL
2	SECURITY
3	OPERATIONS
4	TRAINING

APPENDICES

A	REQUEST FOR ACCESS/WATASO APPOINTMENT LETTER
B	SECURITY BRIEF
C	EMERGENCY ACTION PLAN
D	CLASSIFYING ADP PRODUCTS
E	INFORMAL WIN\TELECONFERENCE MESSAGES
F	FORMAL WIN\TELECONFERENCE MESSAGES
G	PROCEDURES FOR SENDING WINMAIL
H	PROCEDURES FOR RECEIVING WINMAIL
I	PROCEDURES
J	PROCEDURES FOR ENTERING TELECOFERENCE MESSAGE
K	DEPLOYMENT OF WWMCCS TERMINALS

WWMCCS ADP SOP

CHAPTER 1

INTRODUCTION TO THE WWMCCS ADP REMOTE TERMINAL AREA

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	1001	1-3
MISSION	1002	1-3
ORGANIZATION	1003	1-3
RESPONSIBILITIES	1004	1-4

WWMCCS ADP SOP

CHAPTER 1

INTRODUCTION TO THE WWMCCS ADP REMOTE TERMINAL AREA

1001. GENERAL

1. DESCRIPTION OF WWMCCS. The Worldwide Military Command and Control System (WWMCCS) provides the means for operation, direction and technical administrative support involved in the command and control subsystems which enable the National Command Authority (NCA), the Joint Chiefs of Staff and commanders at appropriate subordinate levels to direct and control the operations of U.S. military forces. The elements of WWMCCS are the designated command and control facilities and their associated data collection and processing support, communications, selected warning systems, and execution aids.

2. Reference (n) states that during a crisis and during exercises, unless otherwise directed, the WWMCCS Intercomputer Network (WIN) will be used as the primary means of communications by commands having access to WIN. The missions of the I MEF Operations, Logistics, Planning and C4I2 staffs virtually require that the peacetime staff be trained in and aware of the capabilities of the WIN. All staff members should take an active interest in the WIN as a communications, planning and execution tool.

1002. MISSION. The mission of the WWMCCS ADP remote terminal area at I MEF is three-fold:

1. To assist peacetime planners, logisticians and operators by providing access to data bases and Time-Phased Force Deployment Data (TPFDDs) resident in JOPES and to analyze this information using available retrievals;

2. To provide a means of training a cell of users capable of accessing, sending and retrieving system communications and able to extract deployment execution information from JOPES during contingencies, exercises or crisis action; and

3. To provide a rapid, secure communications medium between CG I MEF and the Joint Planning and Execution Community (JPEC) and other USMC commands for administrative purposes.

1003. ORGANIZATION

1. CG I MEF has one WWMCCS ADP remote terminal area containing two workstations. The Assistant Chief of Staff, G-6 has

WWMCCS ADP SOP

cognizance over the operation and management of the terminal area, as well as providing training to I MEF users. The AC/S, G-6 also has the responsibility for the technical functioning and maintenance of the WWMCCS terminal area. Chief schedules appropriate training for users at the MEF and its MSCs.

a. The AC/S, G-6 assigns in writing the WWMCCS ADP Terminal Area Security Officer (WATASO). The WATASO must be a certified WIN user. Appendix A to this Manual contains a sample appointment letter.

b. The WWMCCS Chief must possess a secondary MOS of 9919, MAGTF Planner.

c. The AC/S, G-6 assigns the ISMO Chief as the WWMCCS ADP Point of Contact (ADPOC). The ADPOC must be a certified WIN user.

2. T/O 4918B assigns six enlisted personnel to the G-6 WWMCCS section to support exercise/contingency planning and execution. These Marines are not required by the section during peacetime. Four of these Marines are assigned to the G-1, G-3, G-4 and G-5, providing administrative augmentation during peacetime. During contingency or exercises, these Marines revert to the control of the G-6 and support the I MEF Crisis Action Team (CAT). These Marines are trained in JOPEs, and must be certified WIN users.

3. One Action Officer each from the G-1, G-3, G-4, G-5 and G-6, represented on the CAT, are trained formally in JOPEs.

4. Personnel designated as WIN users/CAT members must:

a. Possess a Top Secret Clearance.

b. Complete the WIN User's Course (either the three-day resident course held quarterly at CINCPAC or the Computer Directed Training System (CDTS) course resident on the system).

c. Receive the WASSO security brief.

d. Complete and submit, via the WATASO, a WWMCCS ADP System Access Request letter to the WWMCCS ADP System Security Officer (WASSO) at Pacific Operations Support Facility (PACOPSUPPFAC) for approval. Appendix A to this Manual contains a sample WWMCCS ADP System Access Request letter.

1004. RESPONSIBILITIES

WWMCCS ADP SOP

1. WATASO. The WATASO:

- a. Controls access to remote devices.
- b. Assists the WASSO at PACOPSUPPFAC in establishing
- c. Implements the approved security procedures.
- d. Maintains a current access list of personnel authorized unescorted and escorted access to the terminal area.
- e. Reports security abnormalities to the I MEF Security Manager (as appropriate) and the WASSO or his designated representative.
- f. Safeguards and returns ADP products that cannot be identified or contain extraneous data to the WASSO or the WASSO's designated representative.
- g. Conducts random checks of the terminal area to ensure that security requirements are met.
- h. Requests access for users within the organization to the host computers and to other computers in the WIN.
- i. Informs the WASSO when a user's access is no longer required (e.g., PCS) or when data about the individual changes.
- j. Assists the WASSO in issuance of USERIDs and passwords.
- k. Ensures two-party control of any Top Secret output and the Top Secret crypto tape kept in the RTA safe.

2. WWMCCS Chief. The WWMCCS Chief:

- a. Develops, validates and documents information and training requirements for I MEF and its MSCs.
- b. Organizes and manages the daily routine involving the RTA.
- c. Manages and distributes WIN input and output within the CE.
- d. Controls users' or organizations' access to I MEF data files.
- e. Is assigned as the WATASO.
- f. Maintains Desk Top Procedures.

3. ADPPOC. The ADPPOC:

a. Initiates requests for hardware or software support for requirements originating within the command.

b. Participates in the management review of ADP requirements and applications as necessary.

c. Conducts periodic evaluation of ADP applications and systems and makes recommendations for improvements.

d. Revalidates ADP system support.

e. Requests cancellation of contracts when the requirement for maintenance ceases or when the benefits no longer justify the costs.

f. Manages keying and cryptographic requirements.

4. USERS. Each user at I MEF has responsibilities for the security of the WWMCCS terminal and its output. The following list indicates the concerns which all users must show for WWMCCS security and outlines the responsibilities involved. Users must:

a. Protect passwords.

b. Use correct security file and output identifiers and caveats to show the actual classification of data contained in the system or on the output.

c. Control output from the WWMCCS at appropriate security levels.

d. Log off the terminal whenever leaving the terminal to preclude unauthorized use of the terminal by other users.

e. Ensure that only personnel having a need to know and an appropriate clearance see or handle data on the terminal screen or produced from a WWMCCS device.

f. Ensure that the WATASO is advised of any actual or suspected compromise of WWMCCS data, physical security or procedures.

WWMCCS ADP SOP

CHAPTER 2

SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	2001	2-3
ACCESS	2002	2-3
PERSONNEL SECURITY	2003	2-4
PHYSICAL SECURITY	2004	2-4
EMERGENCY DESTRUCTION PLAN	2005	2-5

CHAPTER 2

SECURITY

2001. GENERAL. Security is the highest consideration of the WWMCCS ADP system. A WWMCCS remote terminal operates at the Top Secret level and is safeguarded as such. Users will strictly adhere to the guidelines provided by references (a) through (e) and Chapter 1 and Appendices B and C to this Manual.

2002. ACCESS. The WATASO has direct responsibility for maintaining high standards of security and must be thoroughly familiar with the references and appendices to this Manual. The WATASO controls access to the WWMCCS terminal areas by using a system of "unescorted", "escorted" and "visitor" access levels. Visitors and personnel with escorted access log in and out of a logbook maintained in the terminal area.

1. Unescorted Access. The WATASO grants unescorted access to those people designated as users. A user is an individual who possesses a Top Secret clearance; has a need to know; has been trained per reference (e); possesses a personal USERID/Password; and has read and understands the security brief contained in Appendix B to this Manual.

2. Escorted Access. The WATASO grants escorted access to those CE I MEF Marines based on clearance and need to know. I MEF Marines granted escorted access must have a Top Secret clearance and be escorted into the WWMCCS terminal area by a designated user. The escort briefs the staff member on security procedures as outlined in this Manual.

3. Visitor Access. Visitors are required to log in and out, and must be escorted by a designated user. The escort is responsible for his or her visitor and will never leave a visitor alone in the WWMCCS terminal area. Positive identification of a visitor is mandatory. Check ID cards if personal recognition is impossible. Maintenance workers, system technicians, and guests from other commands are considered visitors. Per reference (a), system technicianb- and maintenance personnel who could affect or modify the security features of the system, or gain access to classified data or information are escorted by the ADPPOC or an appropriately cleared escort who is technically competent to monitor the maintenance work performed.

4. Under no circumstances are staff members with escorted access or visitors allowed to observe the keyboard or monitor

screen during log-on, nor are visitors allowed to operate the WWMCCS terminal unless the WATASO receives documentation requesting access and approves access prior to his or her arrival. The documentation must state the visitor's name, grade, social security number, unit/activity, clearance and access. It also must state the specific nature of the visit.

5. An access roster is posted on the door of the terminal area, in the CDO log book and at the Provost Marshall's Office (PMO) where the alarm system is monitored. In the case of a possible security breach in the terminal area after normal working hours, the CDO notifies those personnel listed as having unescorted access. Should the alarm sound after normal working hours, PMO notifies those personnel listed as having unescorted access.

2003. PERSONNEL SECURITY. People present the greatest risk to and provide the best safeguards for the WWMCCS terminal area. Controlled access, a heightened awareness of the potential risk involved in use of the WWMCCS, and a thorough training program implemented by the WATASO provide a solid foundation for a secure WWMCCS environment. In addition to the guidance provided in Chapter 1 of this Manual, the following measures are employed:

1. Use the system only for authorized purposes. Do not use the workstations as word processors except for output to be entered into the system. Waste, unauthorized use, or misappropriation of the system resources are sufficient causes for the WATASO to revoke access to the WWMCCS terminal area.

2. Maintain individual accountability. The user's access to the system, as well as the user's activity within the system is controlled and open to scrutiny. All transmissions within WIN can be tracked to a particular USERID.

3. NEVER use someone else's personal USERID/password or allow someone else to use yours.

4. Maintain two-person integrity when retrieving Top Secret hard-copy output from the system.

2004. PHYSICAL SECURITY. The WWMCCS terminal area is protected by a series of locks and motion detection alarms. In addition to the guidance set forth in Chapter 1 of this Manual, follow these guidelines:

1. Treat the combinations to the doors, cipher lock, and the safe containing the crypto tape as Top Secret information. Spin

WWMCCS ADP SOP

the combination lock on the door to the terminal area and set the alarm to "secure" after normal working hours.

2. Keep the door to the terminal area closed when using the terminals. Completely screen the terminal area and keyboard against inadvertent observation.

3. Keep on hand some method of physical destruction of the classified hardware contained in the terminal area. A sledgehammer and/or heavy axe are appropriate.

2005. EMERGENCY ACTION PLAN. Emergency destruction will be carried out per I MEFO 5510.5, and Appendix C to this Manual.

WWMCCS ADP SOP

CHAPTER 3

OPERATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
ADMINISTRATION	3001	3-3
MANAGEMENT (DAILY ROUTINE)	3002	3-4
CRISIS ACTION PROCEDURES	3003	3-4
DEPLOYMENT OF WWMCCS TERMINALS	3004	3-5

WWMCCS ADP SOP
CHAPTER 3
OPERATIONS

3001. ADMINISTRATION. The Assistant Chief of Staff, G-6 is responsible for the overall administration and management of the WWMCCS terminal area. Strictly adhere to the following policies:

1. Treat WINMAIL and Teleconference (TLCF) traffic as official correspondence. Distribute them throughout the Command Element (CE) daily just as General Service (GENSER) traffic is distributed. Action officers must ensure format, classification markings and declassification instructions on outgoing WIN traffic are per current directives. Appendix E to this Manual contains the format for informal WIN/TLCF messages. Appendix F to this Manual contains the format for formal WIN/TLCF messages.
2. Maintain master WIN and Teleconference files in the terminal area safe.
3. Do not send WIN traffic, or allow either I MEF users or users from other commands to overwrite files, without notifying the WWMCCS Chief or a designated representative in advance.
4. Do not send WIN traffic or insert files into Teleconference messages without displaying the file in the Timesharing System (TSS) first. The WIN is an official communications medium requiring the same professional standards as any other method of official correspondence. REVIEW YOUR FILE before you send it.
5. The WATASO maintains a log book to document Remote Line Printer (RLP) output. Log in output by Sequential Number (SNUMB) and output date. The WATASO reviews and classifies the output. Users sign for output. The output, if classified, is considered Working Papers for a period of 90 days. At that time, the user who signed for the output either takes it to CMCC to have it controlled or destroys it according to current directives. DESTRUCTION MUST BE REPORTED TO THE WATASO AND LOGGED IN. Users are accountable for all items signed for. Each month, the WATASO reconciles the logbook against user holdings.

3002. MANAGEMENT (DAILY ROUTINE)

1. One enlisted member each from the G-1, G-3, G-4 and G-5 are trained as members of the I MEF Crisis Action Team (CAT) (see paragraph 1003.2). These Marines rotate into the WWMCCS section for on-the-job training to maintain currency. Rotation occurs every seven work days. The training consists of performing

WWMCCS ADP SOP

those tasks required each morning (sending/ receiving WINMAIL/TLCF traffic) and a JOPES lesson taught by the WWMCCS Chief. This training last no more than two hours.

2. The WWMCCS Clerks assigned to the G-6 perform the following tasks:

a. Training as members of the I MEF CAT.

b. Sending files for the CE staff. A File Transfer Service (FTS) message is sent to the I MEF mailbox noting successful transmission of each file. Print this FTS Information Message immediately and give it to the Action Officer who originated the message. Distribute Has Been Sent hard copies as outlined in paragraph (b) below. Appendix G to this Manual contains procedures for sending WINMAIL.

c. Pulling WIN traffic twice daily and Teleconference messages each morning; separating, sorting and properly marking them; routing the WWMCCS Read Board daily to the CE Staff Sections; and distributing private WINMAIL to addressees. Appendix H to this Manual contains procedures for pulling WINMAIL. Appendix I to this Manual contains procedures for pulling Teleconference messages. Appendix J to this Manual contains procedures for entering messages into Teleconferences.

d. Retrieving requested information from JOPES, under supervision of the WWMCCS Chief, for training purposes.

3. The WWMCCS Chief reviews all incoming WINMAIL to ensure proper distribution of personal mail.

4. The WWMCCS Chief assigns file space to each Staff Section. Users store all traffic sent and received by their section in the section's assigned file space.

3003. CRISIS ACTION PROCEDURES During major command post exercises and real world crisis action, the I MEF CAT stands up to support the Battle staff. The CAT consists of JOPES-trained Action Officers and enlisted Marines from each of the general staff sections represented. When the CAT is functioning, the WWMCCS section performs the following functions with the assistance of the JOPES trained action officers and enlisted Marines:

1. Interprets WWMCCS/JOPES information for the Battlestaff.

2. Retrieves needed information from JOPES.

WWMCCS ADP SOP

3. Produces standard and ad hoc JOPES reports.
4. Inputs data, as required, into JOPES data bases.
5. Produces Teleconference transcript files for the Battlestaff.

3004. DEPLOYMENT OF WWMCCS TERMINALS. Appendix K to this Manual contains detailed guidance for deploying WWMCCS.

WWCCS ADP SOP

CHAPTER 4

TRAINING

<u>PARAGRAPH</u>	<u>PAGE</u>	
GENERAL	4001	4-3
ENLISTED USER TRAINING	4002	4-3
ACTION OFFICER TRAINING	4003	4-4
WWMCCS CHIEF'S TRAINING RESPONSIBILITIES PAGE	4004	4-4

WWMCCS ADP SOP

CHAPTER 4

TRAINING

4001. GENERAL. WIN and the Joint Operations Planning and Execution System (JOPES) comprise the means by which I MEF plans and executes the deployment of forces in support of exercises and contingencies. Comprehensive training and aggressive use of the system, and Action Officer awareness of system capabilities will enable I MEF to stand up a qualified, knowledgeable Crisis Action Team.

4002. ENLISTED USER TRAINING. The G-1, G-3, G-4, G-5 and G-6 need an enlisted user responsible for extracting information from JOPES at the request of the Action Officers. They must learn to navigate within JOPES and maintain their proficiency so that they will be ready to stand up with the CAT. Initial training will include:

1. Basic user training in the four WIN subsystems (Time Sharing System (TSS), Teleconferencing (TLCF), TELNET and File Transfer Service (FTS)) includes:

- a. How to log onto the system.
- b. Familiarization with the capabilities of TSS, TLCF and
- c. Navigating between and within the subsystems.
- d. Troubleshooting of minor mechanical problems with the terminal, printer and remote line printer.

e. Sending and pulling WIN and TLCF traffic.

f. How to log off the system.

g. Security procedures.

2. Basic JOPES training, which enables the user to:

a. Pull JOPES standard retrievals.

b. Produce JOPES standard and ad hoc reports.

WWMCCS ADP SOP

C. Input data into JOPES data bases.

d. Determine which JOPES report(s) to provide in answer to a request for information from Action Officers, and how to produce those reports.

4003. ACTION OFFICER TRAINING. The planning data available in JOPES is an enormous source of information pertaining to what this CE does on a daily basis. I MEF AOs must understand what WIN/JOPES can do, not necessarily be familiar with the key-stroke actions required to extract information. Each section needs an Action Officer who can:

1. Understand the levels of detail available in JOPES, including the standard reference files (Geolocation, Ports, Airports, TUCHA, TUDET, etc.).
2. Understand the scope and source of information available in Oplan TPFDDs.
3. Apply this information to questions answerable through WIN/JOPES.
4. Interpret and be familiar with JOPES standard retrievals.
5. Understand the capabilities of WIN and fully utilize it as a communications medium and planning/execution tool.
6. Understand security procedures for WIN and TLCF messages.

4004. WWMCCS CHIEF'S TRAINING RESPONSIBILITIES The WWMCCS Chief:

a. Trains and supervises the G-6 WWMCCS Clerks in the performance of their duties. See paragraph 4002 above.

b. Trains and supervises the enlisted members of the CAT in the performance of their duties, to include a block of JOPES training during each period of on-the-job training. See paragraph 1003 of this Manual.

c. Coordinates, with FMFPAC and HQMC (POC), all WIN, JOPES and related training (including formal school quotas, Mobile Training Teams and guest lecturers) for I MEF and its MSCs.

d. Conducts two days of intensive refresher training for the I MEF CAT members prior to upcoming exercises during which WWMCCS/JOPES will be the primary means of communication/execution.

WWMCCS ADP SOP

e. Coordinates, with PACOPSUPPFAC, student user access to the Computer Directed Training System (CDTS) courses available on the system.

APPENDIX A

REQUEST FOR ACCESS/WATASO APPOINTMENT LETTER

Date: _____

From: _____

Requesting Official's Organization & Code

To: Commanding Officer, Pacific Fleet Data Processing Service
Center, Pearl Harbor (Attn: WWMCCS ADP SYSTEM SECURITY OFFICER
(WASSO))

Subj: REQUEST FOR WWMCCS USERID

1. Request that the following member of this organization be
granted WWMCCS access and/or resources as indicated:

LASTNAME	FIRST	MI	RANK	SSN	PHONE
----------	-------	----	------	-----	-------

2. USERID Request:

a. type: Individual ____ Group ____ Non-Win ____ Win
____ (WSC Apporoval required WSC APPROVAL _____
FOR WIN)

b. Action: (1) Creation (2) Modification (3) Deletion
(4) ADD Group (5) Remove Group (6) Awaiting _____
Reassignment

Enter Staff Code Enter password Change Enter Old User Name or
Userid Date/Time

c.

Highest classification of files to be accessed:

d. If request is for BATCH input only, skip to paragraph 3.

e. UserAccess:

(1) Subsystem Assignments: Highest Urgency: _____
TSS TRAX MOP MDQS CARDIN
TALK UNLOCK _____

(2) Terminal Assignments:

(a) For Access, give terminal ID; i.e., KZ, CY.

(b) For message release authority, enter (R) before the terminal
ID; i.e., RKZ, RCY. (c)

For terminal unlock authority, enter (u) before terminal ID;
i.e., UKZ, URCY.

WWMCCS ADP SOP

WATASO (s) SIGNATURE

3. _____

Type/Printed Name Grade/Title Signature of Requesting Official

Approved by WASSO: Date: _____

WWMCCS ADP SOP

SAMPLE WATASO APPOINTMENT LETTER

5000
G-6/LTR3
DATE

From: Assistant Chief of Staff, G-6
To: Security Manager Pacific Operations Support Facility
(Attn: WASSO)

Subj: APPOINTMENT OF WWMCCS ADP TERMINAL AREA SECURITY OFFICER

Ref: (a) JCS Pub 6-03.7
(b) PACWRAC User's Manual
(c) I MEFO P5230.1

1. Privacy act statement under authority of 5 USC 301. This personal information is requested for appointment as WWMCCS ADP Terminal Area Security Officer (WATASO). Information provided will not be divulged to individuals other than those participating or connected with WWMCCS without your written consent. All personal information not required for system records will be deleted from the system within 60 days after rotation date. You are not required to provide this information, but failure to do so will result in disapproval of your appointment.

2. Effective immediately, the following individual is appointed as the WWMCCS ADP Terminal Area Security Officer (WATASO) for I Marine Expeditionary Force, Camp Pendleton California:

- a. NAME/RANK
- b. SSN:
- c. Security Clearance/Date Final
- d. Organization and Office Symbol:
- e. Installation/Bldg Nr.:
- f. Room Nr:
- g. Duty Phone:
- h. Specimen Signature:

(This letter is submitted to PACOPSUPFAC, Pearl Harbor, Hawaii for formal approval by the WASSO)

WWMCCS ADP SOP
APPENDIX B

WWMCCS ADP SYSTEM SECURITY BRIEFING

1. PURPOSE. The purpose of this briefing is to:

a. Outline, in general terms, the security provisions which have been incorporated into the WWMCCS system.

b. Emphasize individual security responsibilities as they pertain to the WWMCCS system.

c. Provide definitions for some of the more commonly used WWMCCS-specific terms.

2. GENERAL. The security aspects of the WWMCCS system present a new and complex problem involving areas not completely addressed by security directives or procedures. There are no established rules or procedures which can be relied upon to completely protect the ADP system and the classified material which it contains. Therefore, an attempt has been made to incorporate sufficient security provisions into the system, both technical and procedural, to provide adequate protection for material handled.

3. SECURITY CONTROLS. Security provisions have been incorporated into every possible component of the ADP system. These include built-in features in both the system hardware and the software. In addition to technical features, the following physical security provisions have been incorporated into the procedures established for the use of the system:

a. All components of the system, including remote terminals, have been placed in areas secured to a level commensurate with the highest classification of data processed or stored on the system.

b. All users and persons having access to these secured areas must hold clearances commensurate with the highest level of classification contained within the WWMCCS.

c. WWMCCS computer hardware including equipment remotely located must not be moved from the original position without prior evaluation by the WASSO and the Navy Electron Engineering Activity, Pacific (NEEACT PAC). Movement of terminal equipment, even within the reach of the cables (without disconnecting the cable), could result in increased emanation levels. Also the source of power for equipment should not be changed or used for other purposes.

WWMCCS ADP SOP

d. The CARDKEY security access system is one of the primary methods of identifying personnel authorized access to the Pacific Operations Support Facility (PACOPSUPPFAC). A CARDKEY picture pass will be issued to all personnel permanently attached to Pacific Fleet Data Processing Service Center (DPSCPACPH) and personnel from other commands with a recurring need for access to DPSCPACPH. This pass will be automatically validated by the CARDKEY access control system when entering the building, displayed to the Marine Sentry for further verification and will be worn at all times while within DPSCPACPH. This pass will not be worn outside of DPSCPACPH. Personnel are personally responsible for the protection of their pass. Use of another person's pass for any purpose is a security violation punishable by law. Personnel on the DPSCPACPH access list who do not visit regularly will be issued an official visitor's pass. Those personnel not on the local access list will be issued an escort required pass.

e. Entrance to and exit from the Pacific Command WWMCCS Regional ADP Center (PACWRAC) computer site must be through the main doors only. All other doors are alarmed, and an armed guard will investigate any alarm activations. Anyone who is not on the local access list and needs to enter the fifth deck will be issued an escort required badge and will be escorted by personnel from the department to be visited. Only persons on the DPSCPACPH access list will be allowed to enter without an escort. Ensure no one follows you in without checking for access verification from the Marine Sentry.

4. THREATS. There are many threats to this type of system. The more interactive and dynamic the system, the more chances there are for errors which might result in the compromise of sensitive information. These errors could develop in the system's hardware, software or as a result of procedural or human failings. Any error, undetected or uncorrected, may result in a situation where classified information becomes more vulnerable and subject to compromise.

5. INDIVIDUAL RESPONSIBILITIES. The burden of responsibility for the security of classified information within the WWMCCS must ultimately rest with the individual who is using the system. No matter how elaborate the security precautions and safeguards are, they provide little security if the person using the system is not aware of, or does not discharge his/her personal responsibilities. History has shown that it is not the inadequacy of vaults, locks and bars that have been the cause of our nation's security compromises, but rather the human weaknesses of the custodians of our secrets.

WWMCCS ADP SOP

6. ADP SECURITY The following are several areas that directly impact on ADP security associated with the WWMCCS system. program does not exceed the overall classification and special handling caveats of that file.

b. OutPut Security. All system output is considered to be classified to the level of the highest classified data contained within the system until it has been reviewed by an authorized recipient who will verify that the output classification markings and/or special handling banner are correct. If the "DO NOT MARK" (ZZZ) classification code is used, the user is responsible for marking each page of the output with the correct security classification. If you receive output containing extraneous material, notify the WASSO, WATASO or AWATASO and provide the output for futher analysis.

c. Password Security. Remember that the password associated with your USERID is for your eyes only. Do not "lend" your USERID\$PASSWORD combination or "borrow" another' 5 USERID\$PASSWORD. You are held accountable for any security violations associated with your unique USERID\$PASSWORD. For every group USERID\$PASSWORD, a group leader will be identified who will be responsible for the control, distribution, and use of the USERID\$PASSWORD.

d. Security Breaches. All security breaches will be reported immediately to the WWMCCS ADP Terminal Area Security Officer (WATASO) or his designated representative. If a security breach occurs outside normal working hours, a report will be made to the PACWRAC Security Watch who will investigate and report the particulars to the WASSO.

e. Remote Terminal Security. Each terminal area will have a designated WWMCCS ADP Terminal Area Security Officer (WATASO) and one or more Alternate WWMCCS ADP Terminal Area Security Officer(s) (AWATASO) to be available on a 24-hour basis, who will be responsible for the security of the terminal(s) in that area. Remote terminal users will report security breaches to the appropriate WATASO or AWATASO.

(1) Terminal Activation. All terminal users will follow unlock procedures established by the WATASO and WASSO. After the terminal is unlocked, make sure no other person is allowed to observe the terminal keyboard while your USERID and password are being typed in. When logging on a teletype terminal make certain that the teletype overprints the USERID and password in such a manner as to make it illegible or, if the machine fails to do this, obliterate the USERID and password yourself and

immediately notify the WATASO. Additionally, all output containing a USERID\$PASSWORD, even if overprinted, must be disposed of by mulching or in classified bags. When logging on the Video Information Processor (VIP) or Cathode Ray Tube (CRT) terminal that displays the password, ensure that the intensity (brightness) control is turned down.

(2) Terminal Use. Whenever you receive an invalid, inconsistent, or unexpected system response, you should immediately cease operations, sign-off, and notify the computer operator. All hard-copy output removed from the terminal area is to be handled per applicable security procedures and regulations. All Remote Line Printer (RLP) output is to be recorded and signed for on the RLP output record log. Make sure that all hard-copy output which is not to be retained is deposited in the appropriate classified bag. After finishing your work, type in the command BYE or \$*\$DIS and ensure that the message "DISCONNECTS" or "LINE TERMINATED" is the only thing visible on the terminal.

(3) Terminal Status and Securing

(a) Each oncoming operations shift will be briefed on the status of all remote terminals. After normal user working hours, WWMCCS operations will periodically compare the terminals displayed on the video screen with the list of terminals that are not normally manned after normal working hours. When any of those terminals are found active, security will be notified to investigate by monitoring the terminal's activities and determine if the terminal should be locked. If your terminal will be idle for an extended period of time, you should request that the operator lock the terminal.

(b) To secure a remote terminal, a user will contact the PACWRAC Security Watch by phone and request that his remote terminal be locked. After the terminal has been locked, the user will try to sign on. If unable to sign on, the terminal will be considered secured. If the user is still unable to sign on, the WATASO or AWATASO will be consulted to investigate and report the incident to the WASSO. At 1800 (or time assigned your terminal) daily, the computer operator will disconnect all non-24-hour terminals unless the user has specifically requested to the PACWRAC Security Watch extended terminal use. If an extension is required, the WATASO will notify the PACWRAC Security Watch of the approximate time for extended terminal use and the time it will be secured. The WATASO is required to follow up with a message via the appropriate WASO/MESSAGE file or FTS. At the completion of after-hours terminal use, the WATASO will notify the PACWRAC

WWMCCS ADP SOP

Security Watch by phone to disconnect the terminal. Before leaving the terminal area, ensure that all hard-copy output has been detached from the printer and/or that the CRT screen has been cleared, and that the terminals are locked by the PACWRAC Security Watch via the WATASO.

7. GENERAL. As can be seen from the preceding, the individual provides much of the security protection for the information contained in the WWMCCS System. Whether you are a user, a computer operator, programmer, or analyst, if your security alertness is relaxed at any time, a security violation or compromise may result, which could cause grave security. In the final analysis, WWMCCS security, like all security, depends on YOU.

WWMCCS ADP SOP

APPENDIX C

EMERGENCY ACTION PLAN

1. GENERAL. An emergency such as a natural disaster, operational emergency, civil disorder, terrorist threat or casualty emergency could require removing or destroying classified material. The Commanding General, Chief of Staff (or appointed alternate), Security Manager, Adjutant or Command Duty Officer (after working hours) may declare that these situations exist and order the removal or destruction of classified material. An emergency action plan for handling classified WWMCCS material in such situations is required by reference (a). This plan must be understood and readily available to I MEF and Command Duty personnel to effectively remove or destroy such material. The importance of swift reaction cannot be overemphasized.

2. Removal of Classified Material is implemented when an emergency could result in the loss, capture, unauthorized disclosure or compromise of classified material. Removal of material should be considered when protection measures are inadequate and before emergency destruction becomes necessary. Should a situation exist that requires emergency removal of classified material, WWMCCS personnel will be called into the Headquarters. The keying material, all removable hard drives, floppy diskettes, and classified information contained in the Top Secret safe will be transferred to CMCC (Bldg. 1526) for further removal to building 13051, 9th CommBn.

3. Destruction of Classified Material. If any emergency exists during which it is impossible to remove the classified material from I MEF and overrun is imminent, it will be destroyed.

a. Partial (Precautionary) Destruction is the destruction of all COMSEC and other classified material that is not essential to current operations. The primary value of partial (precautionary) destruction, once accomplished, is that if an overrun threat becomes imminent, total (complete) destruction can be completed in a relatively short period of time. If the emergency partial (precautionary) destruction is ordered, WWMCCS personnel will perform the following tasks in order:

(1) Disconnect all WWMCCS equipment from their power

(2) Call the WWMCS floor at PACOPSUPPAC (DSN 88-315-471-8459) and have the terminals rendered inoperable.

WWMCCS ADP SOP

- (3) Destroy the Top Secret crypto tape.
- (4) Destroy all floppy diskettes marked "Top Secret".
- (5) Destroy all hard drive system backup diskettes.
- (6) Maintain a log of all material destroyed.

b. Complete Emergency Destruction is the destruction of all COMSEC and other classified material beyond reconstruction or reuse in the event that an overrun threat becomes unavoidable and classified material cannot be moved to an alternate storage area. In an emergency situation when total destruction of classified material is the specific alternative chosen by the officer directing the emergency action, WWMCCS personnel will:

(1) If partial (precautionary) destruction has not been accomplished, perform the tasks described in paragraph 3.a above.

(2) Locate the sledge hammers stored in the WWMCCS terminal area basement and render all WWMCCS terminal hardware inoperable. The CMS equipment are the first priority.

(3) If time permits, all equipment which could be of use to the enemy, together with pertinent technical, descriptive and operating instructions, will be destroyed or rendered unusable/unrepairable.

(4) All classified material (diskettes, ribbons, TLCF and WINMAIL files) stored in the terminal area will be shredded or burned. After everything has been completely destroyed, report the destruction per paragraph 4 and reference (a) to the appropriate commands.

4. Records and Reports Required. Accurate information concerning the extent of emergency destruction of COMSEC and other classified material is second in importance only to the destruction of the material itself. Log books and control cards will not be destroyed for any reason except to stop them from falling into the hands of the enemy.

a. The facts surrounding emergency complete or partial destruction must be reported to the Chief of Naval Operations (CNO), Director, Communications Security Material System (DCMS), Director, National Security Agency (NSA), with information

WWMCCS ADP SOP

copies provided to CINCPAC, CMC and CG, FMFPAC as soon as possible by the most expeditious means available. Reports should clearly indicate the material destroyed, the method of destruction, and the extent of destruction of items not completely destroyed and which may be presumed to have been compromised.

b. If communications circuits are available, the emergency destruction report will be sent by an IMMEDIATE precedence confidential message.

APPENDIX D

CLASSIFYING ADP PRODUCTS

1. Mark and control all classified documents per references (b) and (c) and the following guidance:

a. Marking. Individuals responsible for controlling the WWMCCS printer mark all banner pages (front and back page of each fan-fold listing) with the classification indicated by the product user.

b. Verification. All users must verify that no extraneous data is included in their output products and that the security classification indicated on the product is consistent with the content. Report all discrepancies to the WWMCCS ADP Terminal Area Security Officer (WATASO). Do not allow printouts with extraneous data to leave the terminal area. Be especially conscious of TLCF transcripts from TLCFs with a TS classification limit. Because TS TLCF messages are relatively rare, they are easy to miss when long transcripts are printed to the RLP on fanfold listings.

c. Controlling. As a minimum, identify all ADP products by the Sequential Number (SNUMB) or other control number and date of creation. Verify and mark the product with the highest classification of any information it contains and protect it accordingly until destroyed. If a classified product is to be released to an activity outside of CE I MEF or placed in a permanent file (to be retained for an indefinite period), or retained more than 90 days, ensure that the product is accounted for, controlled and marked in the manner prescribed in references (b) and (c).

d. Final Markings. After review, mark all printouts with the appropriate classification caveat on the top and bottom of each page (automatically printed by the program, or manually stamped and appropriately page numbered). After reviewing the printout, stamp the first and last pages and front and back covers of the printout at the top and bottom with the appropriate security classification in block letters larger than the printed text. If the system-printed classification marking level (including Unclassified) does not print, stamp the top and bottom of each page with the appropriate classification.

2. TOP SECRET DOCUMENTS. Print Top Secret Documents on the RLP or the page printers in the following manner:

a. Maintain two-person control when printing Top Secret Material in the I MEF terminal area. If only one person with

unescorted access is available, a representative from CMCC will be present.

b. Keep on hand one ribbon for the page printers and one for the RLP for printing Top Secret documents. These ribbons are classified Top Secret.

c. Remove the Top Secret ribbon from the RLP or page printer when printing finishes and store it in the terminal area safe authorized for stowage of Top Secret material.

d. Put Top Secret documents in a Top Secret folder and hand carry them to the CMCC. The CMCC assigns control numbers and distributes them as required.

3. CATHODE RAY TUBE (CRT) DISPLAYS All classified CRT displays must have the appropriate classification marking displayed at the top of the screen. Mark the top and bottom of any page prints made of the CRT display. Follow the instructions above when page printing Top Secret CRT displays.

4. ASSISTANCE. The WATASO provides assistance in determining the proper classification of any ADP product printed in the terminal area.

WWMCCS ADP SOP

APPENDIX E

INFORMAL WIN/TLCF MESSAGES

1. GENERAL. Informal WIN/TLCF messages need not follow any specific format. They may be structured and addressed as convenient for expeditious exchange of information. However, the following elements must be present in the message:

a. Proper classification markings and declassification instructions.

b. To assure clear identification, an informal message shall conclude with the statement:

"THIS IS AN INFORMAL MESSAGE

DRAFTER/RELEASER: (A/O NAME, RANK, POSITION, DSN)"

2. Informal WIN/TLCF messages will not contain command taskings, policy, or be otherwise directive in nature. Short suspense actions received by the CE may warrant soliciting informal comments/recommendations from cognizant Action Officers outside I MEF. Lack of response to an informal query will be taken as "no comment".

WWMCCS ADP SOP

APPENDIX F

FORMAL WIN/TLCF MESSAGES

FROM: CG I MEF//OFFICE SYMBOL//
TO: AUTODIN ADDRESSING//OFFICE SYMBOL(S)//

C L A S S I F I C A T I O N//SSIC//

SUBJ: FORMAT FOR FORMAL WIN/TLCF MESSAGES

REF/A/MTF REFERENCE FORMAT//

1. US MESSAGE TEXT FORMAT WILL BE USED.

DECLASSIFICATION INSTRUCTIONS.

THIS IS A COMMAND COORDINATED MESSAGE.

DRAFTER: (ACTION OFFICER NAME, RANK, DSN)

RELEASER: (APPROVING OFFICER NAME, RANK, POSITION)

WWMCCS ADP SOP

APPENDIX G

PROCEDURES FOR SENDING WINMAIL

1. GENERAL. The following instructions for sending WINMAIL apply to both WWMCCS terminals at I MEF. Some of the procedures (such as preprogrammed function keys) are peculiar to the CE. When operating terminals at other commands, refer to reference (m). All WINMAIL must be formatted per reference (0). All WINMAIL must be dropped to ASCII on a 5 1/4" floppy diskette by the sending section. All system responses below are in bold letters. All user responses are in quotation marks. Do not type the quotation marks.

2. NOTE: Pressing the spacebar and then Xmit is a system "null response". The message NEZT.SCREEN.READY--PLEASE **SPACE AND TRANSMIT** TO RECEIVE...appears at the bottom of every screen where that response is required to bring up the next screen. Always respond correctly to this message.

Log onto the system using "\$5,T53" (PF3).

PLEASE LOG IN

Press function key "PF6"

L -PER NP9IMEF-C -PJ NP9IMEF-C -CAV TZZ -SCC TZZ -Plc

Enter the Top Secret I MEF JCAT password. Press "Xmit"

A government warning paragraph will appear, under which will appear the TSS prompt (*).

*

Place the floppy diskette containing the WINMAIL in drive A.

Press "Alt-F"

The ETC FTFDAC menu will appear, with a pop-up menu superimposed. Using the down-arrow key, place the cursor on the choice reading Workstation Text File to Kost TSS ASCII File
Press "Xmit"

The pop-up menu will disappear. Your cursor will be under the line Sending **File (MB-DOS) Pathname**

Type "A:<name of file on floppy>" Press "Xmit"

Your cursor will be under the line Receiving File (GCOS catalog **file description including UMC**)

G-1
WWMCCS ADP SOP

Type "IMEF/<section's filename in TSS>" Press "Xmit"

The system will tell you that file transfer is in progress, and display the numbers of records and bytes transferred. The system will signal when transmission is complete. Press "Esc"

You will be returned to the TSS prompt (*).

*

Type "DISP IMEF/<section's filename in TSS>" Press "Xmit"

Your file will appear for your review. (DO NOT PROCEED WITH SENDING A FILE THAT CONTAINS ERRORS). The TSS prompt (*) will appear at the bottom of each screen. Press "space Xmit" to review each page. When the file review is completed, type

"JDAC FTS" at the TSS prompt (*). Press "Xmit"

The system will announce that you are in FTS, the version, the date, the time and the host where you are working. You will receive the FTS prompt (=»).

NOTE: If there is mail in the I MEF mailbox that has not been previously read, the following message will appear:

YOU KAVE NEW MAIL

Type "MAIL IMEF/<section's filename in TSS> to <userid you are mailing the WINMAIL to> at <host name where userid is located> CC NP9IMEF-C EXEC PS M" Press "Xmit". For example:

=»MAIL IMEF/MFILE1 TO JCSWINMAIL AT NMCC CC NP9IMEF-C EXEC PS

You have told the system to send your file IMEF/MFILE1 to a mailbox called JCSWINMAIL at the NMCC host, with a carbon copy to the I MEF mailbox. "EXEC PS M" or "EXEC STAT M" tells the system to execute the command, and to monitor, for your viewing, the execution of the command. Always monitor the execution to ensure that the transmission is completed. If a host is unreachable, or if any of the information in your MAIL command is erroneous, the job will abort and the

system will tell you why it was aborted. When the transmission is completed, the FTS mail prompt will appear.

Type "QUIT" Press "Xmit"
The following message will appear

YOU HAVE NEW MAIL

Three messages will have been added to the I MEF mailbox. They are the I MEF carbon copy of the message you have transmitted, an FTS information message stating that your mail was delivered to the addressee, and an FTS information message stating that the I MEF carbon copy was delivered to the I MEF mailbox.

At the FTS prompt (=») type "READ"

The following message will appear.

R=>~MAILBOX CONTAINS (XX) MESSAGES

((XX) equals the total number of messages in the mailbox.)

Type "LIST ALL" followed by the number of the third-to-the-last message, a hyphen, and the number of the last message. Example:

R=~>MAILBOX CONTAINS 6 MESSAGES

"list all 4-6" Press "Xmit"
or, if there are only three messages in the mailbox:

R=>MAILBOX CONTAINS 3 MESSAGES

"LIST ALL"

The three messages described above will appear in order on your screen, with the date/time groups and the size of each message as headings. Page print the FTS information message announcing delivery of the WINMAIL to the addressee for the information of the Action Officer sending the WINMAIL as follows:

With the FTS information message displayed on the screen:

Press "Shift-Print" (a print pop-up menu will appear) and "Xmit"

The FTS information message will be printed to the page printer.

NOTE: To remove any extraneous information from the screen prior

WWMCCS ADP SOP

to printing, place the cursor on that line of text and press "Cntr-Del". The unwanted text will be deleted.

Press "spacebar" then "Xmit" and you will be returned to the FTS READ prompt.

Type "QUIT"

Type "BYE"

*

Type "BYE"

This will log you off of the system; a LINE TERMINATED message will appear at the top of the screen.

NOTE: The system always returns you to the system prompt you logged onto. In this case, you logged onto TSS at the beginning of the session. You cannot log off until you have returned to the TSS prompt (*).

WWMCCS ADP SOP

APPENDIX H

PROCEDURES FOR RECEIVING WINMAIL

1. GENERAL. The following instructions for receiving WINMAIL apply to both terminals at I MEF. Some of the procedures (such as preprogrammed function keys) are peculiar to the CE. When operating terminals at other commands, refer to reference (m). All system responses below are in bold letters. All user responses are in quotation marks. Do not type the quotation marks.

NOTE: Pressing the spacebar and then Xmit is a system "null response". The message NEXT.SCREEN.READY--PLEASE SPACE AND **TRANSMIT** TO RECEIVE...appears at the bottom of every screen where that response is required to bring up the next screen. Always respond correctly to this message.

2. The WWMCCS clerk drops the contents of the I MEF mailbox to a 5 1/4" floppy each morning and again prior to close of business. The mail dropped to floppy in the morning is called a:DDMMM.1 where DD = the date and MMM = the month. The mail dropped to floppy in the evening will be called a:DDMMM.2. The WWMCCS clerk converts the ASCII text of the mailbox to WordPerfect, cleans up the text, prints hard copies, properly marks them, and puts the mail on the WWMCCS traffic board for routing. The WWMCCS clerk also reproduces appropriate copies of the mail as requested by the reviewing officers. The WWMCCS clerk notes the number of messages received in the pass-on logbook maintained in the terminal area.

Log onto the system using "\$5,FTS" (PF4)

PLEASE LOG IN

Press function key "PF6"

L -PER NP9IMEP-C -PJ NP9IMEF-C -CAV ZZZ -SCC TZZ -Plc

Enter the Top Secret I MEF JCAT password. Press "Xmit"

The system will announce that you are in FTS, the version, the date, the time and the host where you are working. You will receive the FTS prompt (=>)

NOTE: If there is mail in the I MEF mailbox that has not been previously read, the following message will appear:

YOU HAVE NEW NAIL

Type "READ" press "Xmit"

R=>>XAILBOX CONTAIN8 (XX) MESBAGE8

((XX) equals the total number of messages in the mailbox).

It is not necessary to review all the messages in the mailbox, only to note the number of messages present.

Type "RSAVE ALL IMEF/WIN~IL" Press "Xmit"

R=> R8AVE SUCCE8BFUL

Type "QUIT" press "Xmit"

Type "DAC TS3" Press "Xmit"

The system will transfer you to the Timesharing Subsystem (TSS) A government warning paragraph will appear, under which will appear the TSS prompt (*)

*

Type "DISP IMEF/WINMAIL" press "Xmit"

All the messages which you reviewed earlier should be displayed. The TSS prompt (*) will appear at the bottom of each screen. Press "space Xmit" to review each page. It is important to review the entire file before continuing to ensure that the entire mailbox has been dropped to the IMEF/WINMAIL file. When you complete the file review, place the floppy diskette to which you will drop the WINMAIL in drive A.

Press "Alt-F"

The ETC FTFDAC menu will appear, with a pop-up menu superimposed. Using the down-arrow key, place the cursor on the choice reading

Host TBS ABCIX File to Workstation Text File

Press "Xmit"

The pop-up menu will disappear. Your cursor will be under the line **8ending File (M8-DoS) Pathname**

Type "IMEF/WINMAIL" Press "Xmit"

WWMCCS ADP SOP

Your cursor will be under the line Receiving File (GCOS catalogi file description including WIC)

Type "a:<DDMMM.X <X = 1 or 2>" Press "Xmit"

The system will tell you that file transfer is in progress, and display the numbers of records and bytes transferred. The system will signal when transmission is complete. Press "Esc".

You will be returned to the TSS prompt (*).

*

Type "JDAC FTS"

The system will announce that you are in FTS, the version, the date, the time and the host where you are working. You will receive the FTS prompt (=>).

Note that the message YOU RAVE NEW MAIL is no longer present. That message only appears when mail is present in the mailbox that has not been previously READ. If the message is present at this point, it means that mail has been delivered to the mailbox while you were in TSS, and you must drop the mail to diskette following the procedures above. If this occurs, the pop-up menu in FTFDAC will permit you to append to the file a:DDMM.X. If you append the new messages to the a:DDMMM.X file, that file will not be overwritten, only added to. if there is no new mail:

Type "PURGE ALL" Press "Xmit"

R=>PURGE TASK WILL BEGIN AFTER QUIT

type "QUIT" Press "Xmit"

R=>PURGE TASK BEGUN; CMID XX SUBMITTED FOR EXECUTION

Type "QUIT" Press "Xmit"

Type "BYE"

This will log you off the system; a LINE TERMINATED message will appear at the top of the screen.

3. Always purge the mailbox following review of the IMEF/WINMAIL file in TSS. Purging the mailbox eliminates the possibility of confusion and simplifies the duties of the next WWMCCS clerk.

WWMCCS ADP SOP

APPENDIX I

PROCEDURES FOR RECEIVING TELECONFERENCE MESSAGES

1. GENERAL. The following instructions for receiving Teleconference (TLCF) messages apply to both terminals at I MEF. Some of the procedures (such as preprogrammed function keys) are peculiar to the CE. When operating terminals at other commands, refer to reference (m). All system responses below are in bold letters. All user responses are in quotation marks. Do not type the quotation marks.

NOTE: Pressing the spacebar and then Xmit is a system "null response". The message NEXT.SCREEN.READY--PLEASE SPACE AND TRANSMIT TO RECEIVE...appears at the bottom of every screen where that response is required to bring up the next screen. Always respond correctly to this message.

2. The WWMCCS clerk reviews all new TLCF messages in the teleconferences monitored by this command, prints hard copies, properly marks them, and puts the traffic on the WWMCCS traffic board for routing. The WWMCCS clerk also reproduces appropriate copies of the TLCF messages as requested by the reviewing officers. The WWMCCS clerk notes the number of messages printed from each teleconference in the pass-on logbook maintained in the terminal area.

Log onto the system using "\$5,TELNET" (PF2).

PLEASE LOG IN

Press function key "PF6".

L -PER NP9IMEF-C -PJ NP9IMEF-C -CAV ZZZ -SCC TZZ -PLC

Enter the Top Secret I MEF JCAT password. Press "Xmit"

The system will announce that you are working in the TELNET subsystem, the version, the date, the time and the host where you are working, and help instructions. You will receive the TELNET prompt (@).

NOTE: TELNET is the subsystem which allows the user to access other Hosts. The teleconferences monitored by I MEF are located at several Hosts, including PACOM. The Host at which each teleconference is located is noted on the Information Board posted in the terminal area. For the purposes of this Manual, the underlined word HOST will be used where an actual Host name should be entered. Remember that you do NOT have to TELNET to PACOM to pull teleconferences located there. You are already at PACOM.

VWMCCSIJOPES TRAINING FOR I MEF CAT

1. BACKGROUND. The WWMCCS Intercomputer Network (WIN) and the Joint Operational Planning and Execution System (JOPES) comprise the means which I MEF plans, executes and monitors the deployment of forces in support of exercises and contingencies. Comprehensive training and aggressive use of the system, Action Officer awareness of system capabilities will enable I MEF to stand up a qualified, knowledgeable Crisis Action Team (CAT). The requirement for a WWMCCS/JOPES conversant CAT was brought painfully home during Desert Shield/Desert Storm.

2. DISCUSSION. The trial-by-error method of training experienced during DS/DS can easily be avoided by training and maintaining the proficiency of a CAT. Members of the CAT should be capable of using WWMCCS/JOPES during crises or during increased operational tempo. These users need to be trained at two levels.by

a. ACTION OFFICER TRAINING. The planning data available in JOPES is an enormous source of information pertaining to what this CE does on a daily basis. I MEF AOs must understand what WIN/JOPES can do, not necessarily be familiar with the key-stroke actions required to extract information. Each section needs an Action Officer who can:

(1) Understand the levels of detail available in JOPES, including the standard reference files (Geolocation, Ports, Aports, TUCHA, TUDET, etc.).

(2) Understand the scope and source of information available in Oplan TPFDDs.

(3) Apply this information to questions answerable through WIN/JOPES.

(4) Interpret and be familiar with JOPES standard retrievals.

(5) Understand the capabilities of WIN and fully utilize it as a communications medium and planning/execution tool.

b. ENLISTED USER TRAINING. Each section needs an enlisted user **responsible for extracting information from** JOPES at the request of the AOs. They must learn to navigate within JOPES and maintain their proficiency so that they will be ready to stand up with the CAT. Initial training will include:

(1) Basic user training in the four WIN subsystems (Time Sharing System (TSS), Teleconferencing (TLCF), TELNET and File Transfer Service (FTS)). This includes:

(a) How to log onto the system.

(b) Familiarization with the capabilities of TSS, Telnet, TLCF AND FTS.

(c) Navigating between and within the subsystems

(d) Troubleshooting of minor mechanical problems with the terminal, printer and remote line printer.

(e) Sending and pulling WIN and TLCF traffic.

(f) How to log off the system.

(g) Security procedures.

(2) Basic JOPES training to enable the user to:

(a) Pull JOPES standard retrievals.

(b) Produce JOPES standard and ad hoc reports.

(c) Input data into JOPES data bases.

(d) Determine which JOPES report(s) to provide in answer to a request for information from Action Officers, and how to produce those reports.

3. RECOMMENDATIONS

a. That one AO from the G-3, G-4, G-5, G-6 and Surgeon attend formal JOPES training. This ten day course consists of a brief WIN overview, a senior officer overview of the Joint Planning and Execution Community (JPEC) and an indepth, hands-on course in the use of JOPES.

b. That one enlisted member from the G-3, G-4, G-5, G-6 and Surgeon attend WIN Orientation Training (a four day in-depth class on the four WIN subsystems described above).

c. That these enlisted members also attend formal JOPES training.

d. That the enlisted members of the CAT maintain their proficiency by rotating, with the WWMCCS clerks, on-the-job training in the I MEF WWMCCS remote terminal area. Ideally, rotation would occur daily; each user would spend approximately 1-2 hours one morning every seven work days performing WWMCCS/JOPES operations.

e. That I MEF promote awareness of the importance of WWMCCS/JOPES proficiency through senior officer attendance at Joint Planning and Operation Courses (JPOC), and by inviting experts in the field to lecture at Camp Pendleton.

Type "OPENH HOST/TLCF" Press "Xmit"

You have asked the system to access HOST and to allow you to work in Teleconferencing (TLCF) at that Host. The "H" after "OPEN" keeps the connection to that Host open after "QUITing" each TLCF at that Host until you have accessed all of the TLCFs you wish to review.

<l4~CONNECTION SUCCESSFUL

The screen will change and the system will announce that you are in TLCF, the version, the date, the time, the Host where you are working and help instructions.

INITIATE, RECONVENE, JOIN, DAC, OR MERGE?

Type "J;<name of teleconference>;NP9IMEF-C Press "Xmit"

Example:

INITIATE, RECONVENE, JOIN, DAC, OR MERGE?J;MCOPSLOG;NP9IMEF-C
"Xmit"

ACCESS GRANTED

Access information will be followed by a series of bulletins announcing the security classification of the TLCF, backup hosts, the number of the latest message entered in the TLCF, and any local or remote print requests pending.

< date time group~ NP9IMEF-C HAS JOINTED THE CONFERENCE COMMAND?
At this prompt, you must note the last message recorded as pulled in the pass-on logbook. For instance, the last message recorded for MCOPSLOG was message number 52. The latest message noted in the TLCF bulletin information is 57.

Type "REVI 53-57" Press "Xmit"

You have asked the system to present for your REVIEW message numbers 53-57. Messages 53 through 57 will appear in order on your screen.

Press "Shift-Print" (a print pop-up menu will appear) and "Xmit"

The screen will be printed to the page printer.

NOTE: Remove any extraneous information from the screen prior to printing. You should remove the **NEXT.SCREEN.READY--PLEASE SPACE AND TRANSMIT TO RECEIVE...** message at the bottom of each screen,

as well as the page number heading on all pages of a message subsequent to the first page. Place the cursor on the line of text you wish to delete and press "Cntl-Del". The unwanted text will be deleted. After each page is printed:

Press "spacebar" and "Xmit"

Remember to form-feed the printer paper when you have printed enough text to complete a page of text.

When you have page printed all the new messages present in the teleconference, you will be returned to

COMMAND?

Type "QUIT"

<O4~PROGRAM TLCF DISCONNECTS
NETWORK CONNECTION STILL OPEN TO HOST
ENTER NEW PROGRAM NAME FOR USE AT HOST
OR ENTER NULL RESPONSE TO CLOSE CONNECTION

If there are more teleconferences you wish to review at this Host, type "TLCF". You will be returned to the INITIATE, **RECONVENE, JOINT**, DAC, OR MERGE? screen, where you will follow the procedures outlined above. If you wish to return to TELNET to open another Host, press "space" the "Xmit". You will be given the TELNET prompt.

Type "OPENH HOST/TLCF" Press "Xmit"

You will then repeat the procedures outlined above for the new Teleconference. When you have finished reviewing all the Teleconferences listed in the pass-on logbook, and have been returned to the TELNET prompt (@):

Type "BYE"

This will log you off the system; a **LINE TERMINATED message** will appear at the top of the screen.

NOTE: Each time you are returned to the TELNET prompt (@), you have been returned to the PACOM Host. If you type "TLCF" at this prompt, you will be Teleconferencing at PACOM.

WWMCCS ADP SOP

APPENDIX J

PROCEDURES FOR SENDING TELECONFERENCE MESSAGES

1. GENERAL. The following instructions for sending Teleconference (TLCF) messages apply to both terminals at I MEF. Some of the procedures (such as preprogrammed function keys) are peculiar to the CE. When operating terminals at other commands, refer to reference (m). All system responses below are in bold letters. All user responses are in quotation marks. Do not type the quotation marks.

2. NOTE: Pressing the spacebar and then Xmit is a system "null response". The message NEXT.SCREEN.READY--PLEASE SPACE AND TRANSMIT TO RECEIVE...appears at the bottom of every screen where that response is required to bring up the next screen. Always respond correctly to this message.

Log onto the system using "\$5,T53" (PF1).

PLEASE LOG IN

Press function key "PF6"

L -PER NP9IMEF-C -PJ NP9IMEF-C -CAV ZZZ -SCC TZZ -PlC

Enter the Top Secret I MEF JCAT password. Press "Xmit"

A government warning paragraph will appear, under which will appear the TSS prompt (*).

*

Place the floppy diskette containing the Teleconference message in drive A.

Press "Alt-F"

The ETC FTFDAC menu will appear, with a pop-up menu superimposed. Using the down-arrow key, place the cursor on the choice reading

Workstation Text File to Host TSS ASCII File

Press "Xmit"

The pop-up menu will disappear. Your cursor will be under the line Sending **File CMS-DOS) Pathname**

Type "A:<name of file on floppy>" Press "Xmit"
Your cursor will be under the line Receiving **File (GCOS catalog1
file description including UMC)**

J-1

WWMCCS ADP SOP

Type "IMEF/<section's filename in TSS>" Press "Xmit"

The system will tell you that file transfer is in progress, and display the numbers of records and bytes transferred. The system will signal when transmission is complete. Press "Esc"

You will be returned to the TSS prompt (*).

*

Type "DISP IMEF/<section's filename in TSS>" Press "Xmit"

Your file will appear for your review. (DO NOT PROCEED WITH SENDING A FILE THAT CONTAINS ERRORS). The TSS prompt (*) will appear at the bottom of each screen. Press "space Xmit" to review each page. When the file review is completed, type "JDAC FTS" at the TSS prompt (*). Press "Xmit"

The system will announce that you are in FTS, the version, the date, the time and the host where you are working. You will receive the FTS prompt (=»).

Type "REPL JCAT/NP9IMEF- AT HOST WITH IMEF/<section's filename in TSS> EXEC PS M" Press "Xmit"

For example, you are going to enter a G-3 message into the MCOPSLOG TLMF at the Host NMCC. At NMCC, just as at all of the Hosts I MEF works with, there is an open filespace called JCAT/NP9IMEF-. You want to get the information contained in the PACOM file IMEF/<section's filename> to a space at NMCC so that you may work with it there. You would type:

"REPL JCAT/NP9IMEF- AT NMCC WITH IMEF/G3 EXEC PS M" Press "Xmit"

You have "replaced" the information contained in JCAT/NP9IMEF- located at NMCC with the information contained in IMEF/G3 at PACOM. "EXEC PS H" (or "EXEC STAT M") tells the system to execute the command, and to monitor, for your viewing, the execution of the command. Always monitor the execution to ensure that the transmission is completed. If a host is unreachable, or if any of the information in your REPL command is erroneous, the job will abort and the system will tell you why it was aborted. When the transmission is completed, the FTS replace prompt will appear.

Type "QUIT" Press "Xmit"

J-2

WWMCCS ADP SOP

Type "DAC TELNET" Press "Xmit"

The system will announce that you are working in the TELNET subsystem, the version, the date, the time, the Host where you are working and help instructions. You will be given the TELNET prompt (~).

Type "OPEN HOST/TLCF" Press "Xmit"

You have asked the system to access HOST and to allow you to work in TLCF at that Host.

<14>CONNECTION SUCCESSFUL

The screen will change and the system will announce that you are in TLCF, the version, the date, the time, the Host where you are working and help instructions.

Type "J;<name of teleconference>;NP9IMEF-C Press "Xmit"

Example:

INITIATE, RECONVENE, JOIN, DAC, OR MERGE?J;MCOPSLOG;NP9IMEF-C
"Xmit"

ACCESS GRANTED

Access information will be followed by a series of bulletins announcing the security classification of the TLCF, backup hosts, the number of the latest message entered in the TLCF, and any local or remote print requests pending.

<date/time group> NP9IMEF-C HAS JOINED THE CONFERENCE

COMMAND?

Type "TALK"

TALK MODE ENTERED IN MCOPSLOG AT MMCC

TIME/DATE

Depending on the setup of the TLCF, you will receive a series of Genser message prompts such as FROM?; TO?; SUBJECT?; etc. Respond to each of these prompts with a "\" "XMIT". You must, however, respond to CLASS? with the appropriate classification (UZZ, CZZ, SZZ, TZZ). You will then be given the TALK mode prompt (>).

Type "\$INSERT JCAT/NP9IMEF-" Press "Xmit"
SPECIAL INSERT INSTRUCTIONS?

WWNCCS ADP SOP

Enter the system null response: spacebar, Xmit.

FILE -- NP9IMEF- -- <XX> LINES INSERTED INTO CURRENT MESSAGE

<XX> is the length of the file you have inserted. Now you want to review your message before you enter it into the TLCF transcript.

Type "\$LIST" press "Xmit"

Your message will be displayed in its entirety. Notice the lines of default Genser prompts you responded to with a "\". These must be removed from the message.

Type "\$EDIT" press "Xmit"

Type "B" press "Xmit"

This backs up your cursor to the first line of the message.

Type \$DELE <XX> press "Xmit"

<XX> is the number of lines you want to delete.

Type "\$LIST" press "Xmit"

Your message will appear again without the header lines. All you will see is the message you inserted into the TLCF. If you are not satisfied with the text, type:

"\$DELE" press "Xmit"

MESSAGE HAS BEEN ERASED BY PARTICIPANT

If you are satisfied with the text, type:

"\$END" press "Xmit"

MESSAGE ACCEPTED

MESSAGE NUMBER <XXX> TIME/DATE BY NP9IMEF-C

<XXX> is the transcript number of your message. Your message has now been officially entered into the TLCF transcript, been assigned a date/time group and a message number. You may read and page print a hard copy of your message by typing:

"\$COMMAND"

WWHCCS ADP SOP

You will be returned to the TLCF command mode.

COMMAND?

Type "REVI <XXX>"

Your message will appear with the TLCF banner line and you can page print the message. At the end of the message TLCF will return you to:

COMMAND?

Type "QUIT" press "Xmit"

You will be returned to the TELNET prompt.

Type "QUIT" Press "Xmit"

The system will close the connection to the Host where you have been working and you will be returned to the TSS prompt.

*

Type "BYE" Press "Xmit"

This will log you off the system.

LINE TERMINATED

WWMCCS ADP SOP
APPENDIX K
DEPLOYMENT OF WWMCCS TERMINALS

1. The MEF needs WWMCCS ADP capabilities during exercise and real world deployments to continue conducting operations planning and reporting. The Joint Staff and senior operational commanders support the use of WWMCCS ADP as a secure, real-time alternative to AUTODIN and include WWMCCS ADP use as a priority exercise objective. I MEF workstations, line printers and associated communications/crypto equipment can be deployed to meet the above objectives.

2. Communications must be established and maintained with a host computer to deploy I MEF WWMCCS ADP successfully. Connectivity into the WWMCCS network normally requires a leadtime of three to seven months. Leased commercial circuits for exercises generally take longer to establish than military/DCS circuits. Under certain circumstances, National Security Emergency Procedures (NSEP) are invoked to provide connectivity on an "as soon as possible" basis. To obtain WWMCCS connectivity, submit a feeder Telecommunications Service Request (TSR) through the operational chain of command six months prior to the requested service date. The I MEF G-6 provides specific instructions regarding TSR preparation.

3. With few exceptions, the following are required to lease commercial service:

a. A 4-wire, full duplex, dedicated line with C2 commercial conditioning and Mil-Std-188C interface.

b. Qualified WWMCCS workstation (IBM WISCUC, Zenith Z248, WWS and modified AN-UYK 85 and Data Products 600 remote line printer. This equipment operates at 2400, 4800 or 9600 bps; however, limit speeds to 4800 bps and below for optimum results.

c. DCS standard signal levels are negative 13dbmO (transmit and receive) at 0db line loss with 600 OHM line termination.

4. The military owned paths available are:

a. Single channel UHF Satellite Communications (SATCOM);
b. Demand Assigned Multiple Access (DAMA);

c. UHF SATCOM; and

d. Ground Mobile Forces (GMF) SHF SATCOM.

9th Communication~ Battalion controls these SATCOM assets and provides coordination and assistance to MAGTF elements requiring access to WWMCCS while deployed. The MAGTF G-6 is normally

responsible for overall coordination and planning for communications connectivity. Implementing details should be in the command and control annex of the OPLAN.

5. DEPLOYED USE OF WWMCCS

a. Deployment Considerations. Employment of WWMCCS workstations requires extensive planning. The items which require greatest lead time include obtaining a port from the supporting host computer, submitting the TSR and coordination with the NAVCAMS or DSC gateway station, as appropriate.

(1) Obtaining a Port. JSC Pub 19 contains detailed procedures for requesting a port at a WWMCCS host computer. I MEF presently uses the USCINCPAC host, located in Hawaii. Deployment of I MEF WWMCCS means that ports must be reallocated from existing connections. When deploying WWMCCS, coordinate additional hardware and port requirements through CG, FMFPAC (G5/G6).

(2) Feeder Telecommunications Service Requests (TSRs). DCA Circular 310-130-1 provides specific instructions regarding TSRs. Connection of a deployed WWMCS terminal to a host can be accomplished through leased telephone service directly between the host and deployed workstation. If the deployed WWMCCS terminal is provided a tactical communications path, via UHF or SHF STACOM, leased telephone service is required between either the NAVCAMS or DCA gateway station involved and the supporting WWMCCS host computer. A Feeder TSR may not be required if either facility has cable links to the host. A correctly prepared TSR for a temporary circuit takes no less than 72 days to process, unless NSEP procedures are invoked.

(3) Coordination with Technical Control Facilities. Technical Control Facility (TECHCON) support is crucial no matter what type of connectivity is required. In a point-to-point leased telephone line link there are TECHCONS at each end of the link and possibly at the commercial carrier's major facilities. In a tactical link, TECHCONS are located at the field sites, the host computer, the gateway station and, if leased lines are used for any portion of the link, at the commercial carrier's major facility. All TECHCONS supporting a deployed WWMCCS terminal must possess the same information regarding the link. This is particularly true for a TECHCON at a link end with the need to route the signal to specific ports or terminals. For WWMCCS operations supported by the PACOM host, the TECHCON is located at NTCC Pearl Harbor, Hawaii. This NTCC also maintains WWMCCS remote transmission hardware including encryption devices, modems and cable accesses to military and commercial leased telephone lines.

b. Considerations Regarding Tactical Connectivity

(1) Single Channel UHF Satellite Communications (SATCOM). UHF STACOM radios associated with WWMCCS operations are the AN/PSC-3, the AN/WSC-3 and AN/WSC-5. The AN/PSC-3 is a portable radio. The AN/WSC-3 is normally installed aboard ship or as a component of the AN/TSC-96. The AN/WSC-5 is a land-based terminal. A WWMCCS synchronous terminal (normal method of data flow) uses a full duplex communications path. This method requires two UHF satellite channels. This is necessary to ensure constant polling and crypto synchronization once the circuit is established. The small number of available UHF SATCOM channels usually preclude the isolation of two channels for WWMCCS unless directed by a CINC. The satellite portion of a UHF WWMCCS link terminates at NAVCAMS.

(2) Demand Assigned Multiple Access (DAMA) UHF SATCOM. DAMA is used to multiplex several signals onto one 250KHz satellite channel. DAMA is installed on many, but not all, Navy ships. If DAMA is used as a communications path for WWMCCS, two full duplex 2400 bps DAMA channels are required: one to send and one to receive. The use of DAMA economizes use of UHF SATCOM channels while allowing improved access to available channels. DAMA usage/channelization is normally determined at the Fleet Commander level. Heavy use of DAMA by the Navy and competition for ports at the host computer make it absolutely necessary that WWMCCS requirements be identified early in the planning cycle. The satellite portion of this WWMCCS link terminates at NAVCAMS.

(3) Ground Mobile Forces (GMF) SHF SATCOM. A GMF transmission path is generally easier to obtain than UHF single channel or DAMA SATCOM. WWMCCS can be placed on a single GMF channel or, if additional multiplexing is available, within a GMF channel. The chance of success is much greater when an entire channel is used. Planning for WWMCCS connectivity must include detailed discussions between operators at the host and DCA (N310). Very specific technical information must be shared among the TECHCON facilities involved.

(4) Shipboard WWMCCS Connectivity. Shipboard SHF connectivity is available on several classes of amphibious ships. Other vessels may be provided with temporary WWMCCS connectivity when a Service component commander is embarked, or when directed by the CINC.