



# UNITED STATES MARINE CORPS

3D MARINE DIVISION (-) (REIN), FMP  
UNIT 35801  
FPO AP 96602-5801

DivO 5271.1B  
G-6

9 JA 2001

## DIVISION ORDER 5271.1B

From: Commanding General  
To: Distribution List

Subj: ELECTRONIC MAIL (E-MAIL) POLICY

Ref: (a) MCO 5271.4  
(b) MCO 5210.11  
(c) MCO P5510.14  
(d) OPNAVINST C5510.93  
(e) SECNAVINST 5216.5  
(f) OPNAVINST 5510.1  
(g) MARADMIN 197-99  
(h) MARADMIN 541/99  
(i) SECNAVINST 5510.36

Encl: 1 E-Mail Policy Statement of Understanding for New Personnel

1. Purpose. To establish policy and provide specific guidance for the administration and use of E-Mail in accordance with references (a) through (i). This Order is punitive in regard to paragraphs 4j, 4k, and 4l, and violations are punishable under Article 92, UCMJ.

2. Cancellation. DivO 5271.1A.

3. Background. The Division has two Local Area Networks (LAN), classified and unclassified. The unclassified LAN is connected to the Defense Information System Network (DISN) via the Okinawa Wide Area Network (OWAN). This connection provides Division organizations access to the worldwide capabilities of the Non-secure Internet Protocol Router Network (NIPRNET) including Internet access. The classified LAN is connected to the Secure Internet Protocol Router Network (SIPRNET), and also has secure worldwide connectivity. Except where noted, this order applies to both 3d Marine Division LANs.

#### 4. Definitions

a. Non-Secure Internet Protocol Router Network. NIPRNET is a non-secure network. NIPRNET is authorized to process UNCLASSIFIED traffic only.

9 JAN 2001

b. Secure Internet Protocol Router Network. SIPRNET is a secure network. SIPRNET is authorized to process traffic up to the SECRET level. SIPRNET users must have at least a SECRET clearance.

c. Electronic-Mail. E-Mail is an authorized means of communication that uses computer-to-computer data transfer technology, normally in the form of textual messages or attached data files.

d. Virus Protection

(1) Protection. Norton Anti-Virus is the standard Anti-Virus software used by the 3d Marine Division and is resident on the Server Management Server (SMS). Upon logon, SMS verifies that the most current Anti-Virus software has been installed on the individual's workstation. If SMS detects that the anti-virus patch is outdated, it will install the updated version. There is no user intervention required. Users should not attempt to download patches directly from the internet.

(2) Detection. Users who contract a virus that is not detected by Norton Anti-Virus should contact the G-6 immediately. Users should not attempt to inoculate the virus themselves nor should they open attachments they suspect to be infected as this can result in further dissemination of the virus.

(a) When reporting a virus, the following information is required:

- 1 Name of the virus.
- 2 Date and time detected
- 3 Suspected source of the virus.
- 4 Actions taken to remove/isolate the virus.

(3) If a user activates a virus, that mailbox will be immediately deleted and the computer removed from the Marine Corps Enterprise Network (MCEN). That mailbox will not be recreated until the supporting S-6 or G-6 has inspected the computer to ensure that the virus has been removed. Some computers may require reformatting depending on the string of virus activated.

e. Organizational E-Mail. Organizational E-Mail is any message or file transmitted to or from an authorized organizational mailbox. Organizational E-Mail is the most formal type of E-Mail sent to or from an organization in the name of the commander. This is comparable to traditional formal correspondence or message traffic addressed by title to the commander of an organization.

f. Organizational Mailbox (OMB). The OMB is the E-Mail address of an office, activity, or command authorized to send and receive organizational E-Mail. Only those offices, activities, and commands with a Plain Language Address (PLA) are authorized an OMB. More than one person may access this mailbox, as authorized by the commander or head of the office owning the mailbox. The LAN profile for the OMB will allow only authorized users access to the E-Mail and printer services. Organizations will monitor their mailboxes and ensure that appropriate action is taken on incoming E-Mail.

g. Section E-Mail. Section E-Mail is any message or file transmitted to or from a section's mailbox.

h. Section Mailbox(SMB). The SMB is an E-Mail address of a subordinate office, activity, or element of a command. Such offices are not authorized an OMB. More than one person may access this mailbox, as authorized by the commander or head of the office owning the mailbox.

i. Individual E-Mail. Individual E-Mail is a message or file transmitted to or from an individual's mailbox containing informal information that does not commit or direct an organization. The intent of individual E-Mail is to facilitate the direct exchange of information in much the same manner as the telephone. The Security Manager will consider requirements for individual classified accounts on a case-by-case basis.

j. Individual Mailbox. The individual mailbox is the E-Mail address of an individual. In accordance with established security procedures, access to this mailbox is limited to the individual whose name is on the account. Marines cannot authorize an individual to check their E-Mail while they are absent. Passwords will expire and must be changed every 90 days.

k. Official Use. Marine Corps information technology resources can be used when work related and determined to be in the best interest of the federal government and the Marine Corps. Access should be appropriate in frequency, duration, and be related to assigned tasks. Examples include using the Internet to:

(1) Obtain information to support Department of Defense, Department of the Navy and United States Marine Corps missions.

(2) Obtain information that enhances the professional skills of Marine Corps personnel.

(3) Improve professional or personal skills as part of a formal academic education or military/civilian professional development program (if approved by the command).

9 JAN 2001

1. Authorized use. The limits of authorized use may vary from command to command depending on the strength of the network and command information needs. Under optimum conditions, Marine Corps computers may be used to access the Internet for incidental personal purposes such as Internet searches and brief communications as long as such use:

(1) Does not adversely affect the performance of official duties by the Marine/Employee.

(2) Serve a legitimate interest such as enhancing professional skills or improving morale.

(3) Is of minimal frequency and duration and occurs during an individual's personal time.

(4) Does not overburden Marine Corps computing resources or communication systems.

Does not result in added costs to the government.

(6) Is not used for purposes that adversely reflect upon the Marine Corps

(7) The exchange of personal, unofficial E-Mail between Marine Corps Enterprise Networks (MCEN) and commercially hosted accounts (i.e., sending a personal E-Mail message to your family at their @ATT.COM E-Mail address from your MC E-Mail) account is authorized if in accordance with reference (f).

m. Prohibited Use. Use of Marine Corps resources to connect to the Internet for purposes other than those described in paragraphs 4j and 4k above is prohibited. These prohibited activities may result in administrative or other disciplinary action such as courts-martial or non-judicial punishment. Examples of prohibited use include, but are not limited to the following:

(1) Illegal, fraudulent, or malicious activities

(2) Partisan political activity, political or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps or DOD.

(3) Activities whose purposes are for personal or commercial financial gain. These activities include solicitation of business services or sale of personal property.

9 JAN 2001

- 4) Unauthorized fundraising.
  - (5) Accessing, storing, processing, displaying or distributing offensive material such as pornography or hate literature.
  - (6) Obtaining, installing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.
  - 7 The creation, forwarding, or passing of chain letters.
  - (8) Accessing (logging into) commercial E-Mail services via WEB interface (e.g., hotmail.com, aol.com, att.net, etc.) from the (Marine Corps Enterprise Network (MCEN) is not authorized.
  - (9) Under no circumstances will official government correspondence or data files be sent or forwarded to, or created or stored on, commercial E-Mail services (WEB enabled or otherwise).
- n. Authorized Software. Authorized software is computer software, to include programs and data, which is authorized for use on government computer systems. Program software includes applications and utilities that are either purchased or licensed for government use. Data includes data of any type that is purchased or licensed for government use, or created for official use or authorized use. Software, which does not require licensing, such as public domain software, or "freeware", is authorized if used for official or authorized usage and approved by the Division Information Systems Management Officer (ISMO).
- o. Unauthorized Software. Unauthorized software is computer software, to include programs and data, which does not meet the criteria of authorized software.
- p. Working Papers. Working papers include classified notes from a training course or conference, research notes, drafts, document downloaded and saved to disk from the SIPRNET and similar items that are not finished documents.

5. Management. E-Mail management is a command responsibility. Users will manage their individual mailboxes in accordance with the following guidelines:

- a. When feasible, mailboxes (OMB, SMB, and individual) will be checked for new mail at least twice during the workday. Additionally all mailboxes will be reviewed a minimum of once per month to purge, retain, or file E-Mail as appropriate.

9 JAN 2001

b. Users will aggressively monitor their individual mailboxes, so as not to exceed their mailbox limit. The limit for a mailbox is (20) twenty megabytes. Personnel who habitually exceed their mailbox limit will be subject to loss of account privileges. Users are encouraged to use their personal folders to store mail. Mail stored in personal folders does not count against mailbox limits. Instructions for configuring personal folders can be found at <http://www.3div.usmc.mil> in the Self-Training and Help link.

c. Users who are TAD or on leave for extended periods (five days or more) should arrange to check their mailboxes periodically, either through forwarding of E-Mail to their temporary location, Remote Access Server/Virtual Private Network (RAS/VPN) or the 3d Marine Division Web Access Client. The G-6/S-6 or ISC will provide further assistance as required.

d. Enclosure (1) will be incorporated into the check-in process for Division organizations as a means of ensuring that newly arrived Marines requiring access to the NIPRNET/SIPRNET understand the provision of this Order. New personnel will read and sign enclosure (1) signifying understanding. The G-6/S-6 or ISC will retain a signed copy of enclosure (1) until the account is disestablished and/or the individual transfers from the Division.

6. Security. It is the responsibility of the E-Mail user to safeguard the information transmitted/received and protect it based on its sensitivity level (i.e., sensitive, unclassified, and classified) per references (c) and (d). In addition users requiring SIPRNET accounts must read and sign the Information Assurance package.

a. Shared files and public folders are to be treated as public drives with no expectation of privacy. Sensitive information such as counseling notes and fitness reports are easily accessible unless the owner has made specific arrangements with the G-6/S-6 or Information Systems Coordinator to limit access to these files. The owner still bears the responsibility for their inadvertent public disclosure. This type of information should be saved/stored on floppy disk and protected by the owner.

b. The users will safeguard individual E-Mail accounts. The G-6/S-6 or ISC will disestablish accounts of personnel detaching the command upon transfer. This will be facilitated by incorporation of the G-6/S-6 or Information Systems Coordinator (ISC) into the checkout process.

c. Account passwords will be changed at least once every (90) ninety days. Passwords should be chosen with care. Utilizing an unlikely combination of alphabetic characters, numbers, and punctuation provides greater protection from password-sniffer and

9 JAN 2001

dictionary based cracking programs. Passwords MUST not be written down.

### Release of Naval Message Traffic

a. General. The primary function of Message Dissemination Subsystem (MDS) Multiple PLA Editions with Profiler and E-Mail Link is the automatic dissemination of organizational Naval message traffic to various offices as MDS users or E-Mail addressees. This dissemination is based on Plain Language Addresses (PLAs), Command Guard List (CGL) entries, and Special Handling Profiles. MDS is a software application that resides on a LAN file server. Messages are made available to MDS for distribution via Marine Corps Base Camp Butler Telecommunications Center Message Routing System (MRS).

b. Establishing an Account/Authorization to Use. MDS user accounts are established by e-mail authorization with access given through Microsoft Outlook folders. G-6/ISMO is ultimately responsible for all access given to the MDS folders. S-6/ISMOs are responsible for ensuring users have need to know for Special Handling folder access.

c. Plain Language Addresses (PLAs). The Base Telecommunications center MRS routes messages to the Division MDS according to PLA. The Third Marine Division is responsible for all of the Division Major Subordinate Elements (MSEs) and their Unit Deployment Programs (UDPs) on Okinawa. The Division MDS is in current revision of PLAs due to the UDP rotation schedule. It is the responsibility of the Regimental S-6/ISMO to coordinate with incoming UDPs the Naval Message traffic needs of their unit, and pass on to the Division G-6 the results of the inquiry.

d. Command Guard List (CGL) entries. Command Guard List entries consist of Address Indicator Groups (AIGs) and Collective Address Designators (CADs). The MDS maintains a listing of the CGLs that the various units within the Division are members of and route messages to public folders according to that list. The CGL entries are constantly changing as units are added to and removed from AIGs and CADs. UDP's are responsible for ensuring that CGL information is provided on the Command Guard Shift (Commshift).

e. All message (ALLMSG) and Special Handling (SPEC HAND) Profiles. Messages are distributed throughout MDS by the use of profiles. Profiles are key words or phrases that may form a subject identical to those listed in a message that the software will search for. Most profiles fall under a special handling category. Such profiles are personal for Substance Abuse Control Officer's (SACO) messages, Personnel Casualty Reports (PCRs), and Serious Incident Reports (SIRs). All other messages are automatically routed to each

9 JAN 2001

unit's ALLMSG folder, which is determined by the PLA and/or CGL that the message falls under.

f. Operating Procedures. The Marine Telecommunications Center (MTCC) Camp Butler provides Naval telecommunications service for the CG, III Marine Expeditionary Force, 3d MarDiv, and all units/sections located on Okinawa. As message traffic comes into the MTCC it is routed to MDT (Message Distribution Terminal). MDT then separates classified from unclassified message traffic and passes the message traffic to the Gateguard program. Gateguard ensures that the messages meet the classification authorized for transmission over that network and then distributes the message traffic to the Message Routing System (MRS). MRS then routes the message traffic via the Windows NT Network to the Division G-6/ISMO Message Dissemination Subsystem (MDS), which routes messages to public folders located in Microsoft Outlook.

g. Drafting/Sending Messages. Messages are drafted per instructions contained in Naval Telecommunications Publication 3(I) and the current edition of Message Text Format Editor Software. Ensure that all PLA's are valid by running the current Distributed Plain Language Address Verification System (DPVS) data base program before a message is sent to MTCC Camp Butler. After messages are drafted in the MTF format, each section sends their messages to the MTCC Camp Butler via a section (OMB) for transmission. The outgoing messages are sent as E-Mail attachments. The precedence and DTGs are included in the subject line of the E-Mail. Each E-Mail sent is certified for proper accountability. Sections must ensure that messages are properly screened before released to the MTCC.

h. Receiving Messages. MTCC provides automatic distribution of message traffic to all outlying units via the Windows NT network. The Division G-6/ISMO MDS routes all incoming messages to selected users.

i. Location of Message Files/Recovering Old Messages. Message traffic is electronically stored for a period of 10 days in the "All Messages" folder located under the 3Div/Staff/Staff MDS folder. Messages older than 10 days are moved to the "Staff History MDS" where they are stored for 12 months.

## 8. Classified Message Traffic

a. Secret/Confidential Messages. As established in the current edition of reference (f), Confidential and Secret messages no longer require a signature at the communications center. Staff sections are required to establish procedures for control and destruction of all classified messages in their custody.

b. Top Secret Messages. Top Secret messages will be delivered to the Top Secret Control Officer (TSCO) for distribution. All copies will be numbered and signed for.

9 JAN 2001

## 9 Messages Requiring Special Handling

a. Special Category (SPECAT) Messages. SPECAT messages are always classified. These messages will be handled according to their classification and in accordance with specific written instructions provided by the designated control officer for the "code word" message.

b. During working hours, SPECATs will be handled as directed by the control officer. After working hours, SPECATs will be handled per paragraph 9e below. All top secret SPECATs will be handled per subparagraph a above.

c. Limited Distribution (LIMDIS) Messages. LIMDIS messages will be distributed per the current edition of Division Order P2130.1. Distribution of LIMDIS messages will be to the staff section having primary staff cognizance as indicated in the current edition of DivO P2130.1.

d. Personal For. "Personal For" messages will be electronically routed to the "Personal For" folder in Microsoft Outlook. The Commanding General, Chief Of Staff, Adjutant, and Staff Secretary have access to this folder.

e. After Working Hours. After working hours, the MTCC will notify the Command Duty Officer (CDO) of receipt of messages requiring special handling.

10. Authorized E-Mail Software. The Division E-Mail software standard is Microsoft Outlook 97 or 98.

11. Retention Policy for Classified Documents Downloaded from the SIPRNET.

a. As established in the current edition of reference (i) Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents. Working papers that contain classified information shall be:

(1) Dated when created

(2) Conspicuously marked "Working Paper" on the first page in letters larger than the text.

(3) Marked centered top and bottom on each page with the highest overall classification level of any information they contain.

(4) Protected per the assigned classification level.

9 JAN 2001

Destroyed, by authorized means, when no longer needed

b. Commanding officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator.

12. Action

a. Assistant Chief of Staff, G-6 (AC/S, G-6)

(1) Manage all E-Mail accounts.

(2) Install and maintain the OMB for 3d Marine Division.

(3) Coordinate with the appropriate S-6/ISC for creation of OMB's and SMB's for all appropriate Division organizations and units.

(4) Provide technical support and assistance to the Division Staff and organizational S-6/ISC's as required to implement the provisions of this Order.

(5) Ensure that the contents of this order are included in the Division's Logistical Readiness Inspection program.

b. Commanding Officers, Regiments and Separate Battalions

(1) Assign OMB/SMB coordinators.

Operate your OMB/SMB in accordance with this Order

(3) Incorporate enclosure (1) into the unit check-in process of those Marines that require access to the LAN.

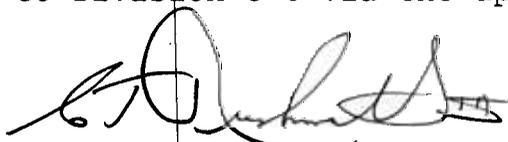
(4) Ensure that the G-6/S-6 or ISC is incorporated into the unit check-in/out process to facilitate the establishment/disestablishment of E-Mail accounts.

Implement the provisions of this Order.

(6) Commanding officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator (paragraph 11 refers).

DivO 5271.1B  
9 JAN 2001

13. Recommendations. Recommendations for changes to this Order are invited and should be submitted to Division G-6 via the appropriate chain of command.

A handwritten signature in black ink, appearing to read 'C. T. Rushworth III', written in a cursive style.

C. T. RUSHWORTH III  
Chief of Staff

DISTRIBUTION: A/D