



UNITED STATES MARINE CORPS
MARINE CORPS BASE
QUANTICO, VIRGINIA 22134-5001

MCBO 5230.3
B 054
20 JAN 2000

MARINE CORPS BASE ORDER 5230.3

From: Commanding General
To: Distribution List

Subj: INTERNET ACCESS AND ELECTRONIC MESSAGING

Ref: (a) MCO 5271.4A
(b) DoD 5500.7-R
(c) ALMAR 167/97
(d) MARADMIN 197/99
(e) MARADMIN 541/99

Encl: (1) Information Assurance (IA) Administrative Framework
(2) Notice and Consent Log-On Banner

1. Purpose. To establish individual duties and responsibilities regarding the proper use of U.S. Government Information Systems to access the Internet and use of electronic messaging (e-mail). This Order is punitive and applies to DoD employees and Defense Contractors who utilize Government Information Systems.

2. Cancellation. MCBO 5510.2.

3. Background

a. The Marine Corps Enterprise Network (MCEN), which is a subset of the Defense Information Systems Network (DISN), interconnects Marine Corps commands and activities, per reference (a). A complex system of network operating systems and application software allows commands and activities to exchange information over MCEN and obtain access to other computer networks, such as the Internet.

b. MCB, Quantico is interconnected with other military commands via the MCEN and DISN. The data network infrastructure aboard Quantico is a valuable resource that provides users with services such as e-mail and directory services, naval messaging distribution, and access to Internet resources. This connectivity and the government computer systems make it easier for personnel aboard MCB, Quantico to conduct official business.

20 JAN 2000

c. The MCEN has limits to the number and types of information files (text, pictures, etc.) it can transport. Too many users simultaneously sending and/or receiving large files will potentially degrade network performance and deny access to other official Internet users. These conditions demand we discipline our use of the network with regard to both the size of files we transmit and receive when using Marine Corps assets to access the Internet. Reference (b) permits using government information systems for official use and other authorized purposes as listed herein.

4. Definitions

a. Information Systems (IS). IS are any telecommunications and/or subsystem used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, video imagery, video teleconferencing, messaging, or data, to include software, firmware, and hardware.

b. Command Information Systems Security Manager (CISSM). The CISSM is a field grade officer or civilian manager in the grade of GS-11 and above who serves as the principal advisor on all automated systems security measures, to include personnel, access, physical security, communications, emanations, hardware, and software. The Command Security Manager will also serve as the CISSM. Relationships for the CISSM and other Information Systems Security personnel are depicted in enclosure (1).

c. Assistant Information Systems Security Manager (AISSM). The AISSM coordinates the information assurance (IA) computer security program for MCB and MCCDC. Serves as the focal point for investigation and resolution of IA computer security violations and/or incidents. Assists in the management of computer risk management, security, and contingency planning programs at MCB/MCCDC Quantico.

d. Information Systems Security Officer (ISSO). Each major organization or command (i.e., MCCDC, T&E, MCU) will have an ISSO appointed as an additional duty. The ISSO will ensure local compliance with computer security operating procedures and that every computer within their respective organization displays the warning banner contained in enclosure (2) at the first point in the log-in process, per reference (c). Computer security violations and/or incidents will be reported by the ISSO to the CISSM via the AISSM and appropriate chain of command.

20 JAN 2000

e. Information Systems Security Coordinator (ISSC)/Terminal Area Security Officer (TASO). An ISSC/TASO will be appointed for each division/branch. The ISSC/TASO is the end-user's first point of contact for computer access and questions.

f. User. A user is an individual, person or process authorized to access an IS. Users are responsible for ensuring the security of the IS and the information processed. All IS users will:

(1) Coordinate computer access, questions, and problems with appropriate ISSC/TASO.

(2) Read and comply with paragraph 5 of this Order regarding official use, authorized use, and prohibited use of Marine Corps resources when using the Internet and e-mail.

(3) Use a password protected screensaver, lock the workstation, or log off when leaving the computer unattended.

(4) Protect passwords from compromise.

(5) Log off the Internet when connection is not actively utilized.

(6) Report all discrepancies and infractions of this Order to the appropriate ISSO/ISSC or to the CISSM.

g. DoD Employee

(1) Any DoD civilian officer or employee (including special Government employees) of any DoD component (including any non-appropriated fund activity).

(2) Any active duty Regular or Reserve military officer, including warrant officers.

(3) Any active duty enlisted member of the Army, Navy, Air Force, or Marine Corps.

(4) Any Reserve or National Guard member on active duty under orders issued pursuant to title 10, United States Code.

(5) Any Reserve or National Guard member performing official duties, including while on inactive duty for training or while earning retirement points, pursuant to title 10, United States Code, or while engaged in any activity related to the performance of a Federal duty or function.

20 JAN 2000

(6) Any faculty member in a civil service position or hired pursuant to title 10, United States Code, and any student (including a cadet or midshipman) of an academy, college, university, or school of DoD.

(7) Consistent with labor agreements and international treaties and agreements, and host country laws, any foreign national working for a DoD Component except those hired pursuant to a defense contract.

h. Defense Contractor. Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with DoD or a DoD Component to furnish services, supplies, or both, including construction. Subcontractors are excluded unless they are separate legal non-Federal entities that contract directly with DoD or a DoD Component in their own names. Foreign governments or representatives of foreign governments that are engaged in selling to DoD or a DoD Component are defense contractors when acting in that context.

5. Policy

a. U.S. Government IS are authorized for official use and authorized purposes only. Unauthorized use of these systems violates U.S. Government regulations, subjecting individuals to appropriate administrative and judicial action.

b. Official Use. Marine Corps resources that provide access to Internet services can be used for work related functions, when determined to be in the best interests of the U.S. Government and the Marine Corps, per reference (d). Access should be appropriate in frequency, duration, and be related to assigned tasks. Examples of official uses are:

(1) To obtain information to support DoD/DON/USMC missions.

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

(3) To improve professional or personal skills as part of a formal academic education or military/civilian professional development program, when approved by the chain of command.

c. Authorized Purposes/Use. Under optimum conditions, employees may use Marine Corps computers to access the Internet for incidental personal purposes such as Internet searches and brief communications as long as such use:

20 JAN 2000

(1) Does not adversely affect the performance of official duties by the employee.

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

(3) Is of minimal frequency and duration and occurs during an individual's personal time (i.e., off-duty hours, lunch time, etc.).

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

(5) Does not result in added costs to the Government above normal operating expenses.

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

d. Prohibited Use. Use of Marine Corps resources to connect to the Internet for purposes other than those described in paragraphs 5.b. and 5.c., above, is prohibited. The following are examples of prohibited Internet uses:

(1) Introducing classified information into an unclassified system.

(2) Storing, accessing, processing, or distributing classified, proprietary, sensitive, "For Official Use Only", or Privacy Act protected information on a computer or network not explicitly approved for such processing.

(3) Accessing/logging into commercial e-mail services via web interface (e.g., hotmail.com, aol.com, att.net, etc.) from within the MCEN. Furthermore, under no circumstances will official government correspondence or data files be sent to, forwarded to, created or stored on commercial e-mail services (web enabled or otherwise). This includes, but is not limited to, formal message traffic (e.g., Message Dissemination Subsystem), working documents and all official e-mail. Reference (e) provides additional guidance on this matter.

(4) Accessing, storing, processing, displaying, distributing, transmitting or viewing material that is pornographic, sexist, racist, promotive of hate crimes, or subversive in nature. This includes accessing pornographic web sites, sending or receiving e-mails with pornographic file attachments, and utilizing lewd or sexually suggestive screen savers and wallpaper.

20 JAN 2000

(5) Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

(6) Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software code, to include viruses, logic bombs, worms and macro viruses.

(7) Activities whose purposes are for commercial financial gain.

(8) Illegal, fraudulent, or malicious activities.

(9) Fund-raising not authorized by reference (b).

(10) Gambling, wagering or placing of any bets.

(11) Writing, forwarding or participating in chain letters, suspected virus warnings, and/or hoaxes.

(12) Posting personal home pages.

e. Audio and/or Video Data Streaming. Audio and/or video data streaming is the process by which users access live radio or television programs through the Internet. Data streaming consumes valuable bandwidth in a constant state throughout the duration of the broadcast, places an unnecessary burden on the network infrastructure, and degrades network performance in support of official government business. Audio and/or data streaming is not considered permissible access to the Internet and is prohibited under the policy set forth in reference (d).

f. All users are reminded that they have no expectation of privacy in using Government IS. Use of Government IS, including use of the Internet and e-mail, is subject to monitoring, interception, accessing and recording, and may be passed to law enforcement. Any violation of paragraphs 5.b. through 5.e. above can result in disciplinary or administrative action.

6. Guidance

a. All users with access to the MCB, Quantico network will be assigned a unique Internet Protocol (IP) address. The IP address will allow receipt of both e-mail and official message traffic, as well as Internet access. Internet access may be revoked on a case-

20 JAN 2000

by-case basis at the discretion of supervisors, division directors, or higher authority. If use of the Internet is essential to performing assigned duties and responsibilities, loss of access may have an adverse impact on continued employment in that position.

b. Commanders, directors, and OIC's will enforce this policy, and will appoint an individual to serve as their organization's ISSC/TASO. They also will ensure all personnel within their organization who are granted access to IS are aware of the contents of this Order, and have access to pertinent regulations, as required. The President, MCU, is authorized to develop procedures for student Internet access, as required for instruction.

c. The CISSM will conduct IS surveys, with assistance from G-6 Division and Marine Corps Information Technology and Network Operations Center. When identified, incidents and misuse will be reported to the CISSM and investigated through the Naval Criminal Investigative Service. Results of the inquiry will be forwarded to the unit commander for military personnel, or division director for civilian personnel, for administrative or legal action. Copies of written statements made by a civilian employee who is under investigation will be provided to the employee or the employee's representative, per applicable negotiated agreements or civilian personnel regulations.

d. The AC/S, G-6 will:

(1) Assist the CISSM in conducting random network surveys aboard MCB, Quantico and provide technical support in the form of personnel and equipment, as needed.

(2) Ensure instruction on proper Internet use is included in all local computer training classes.

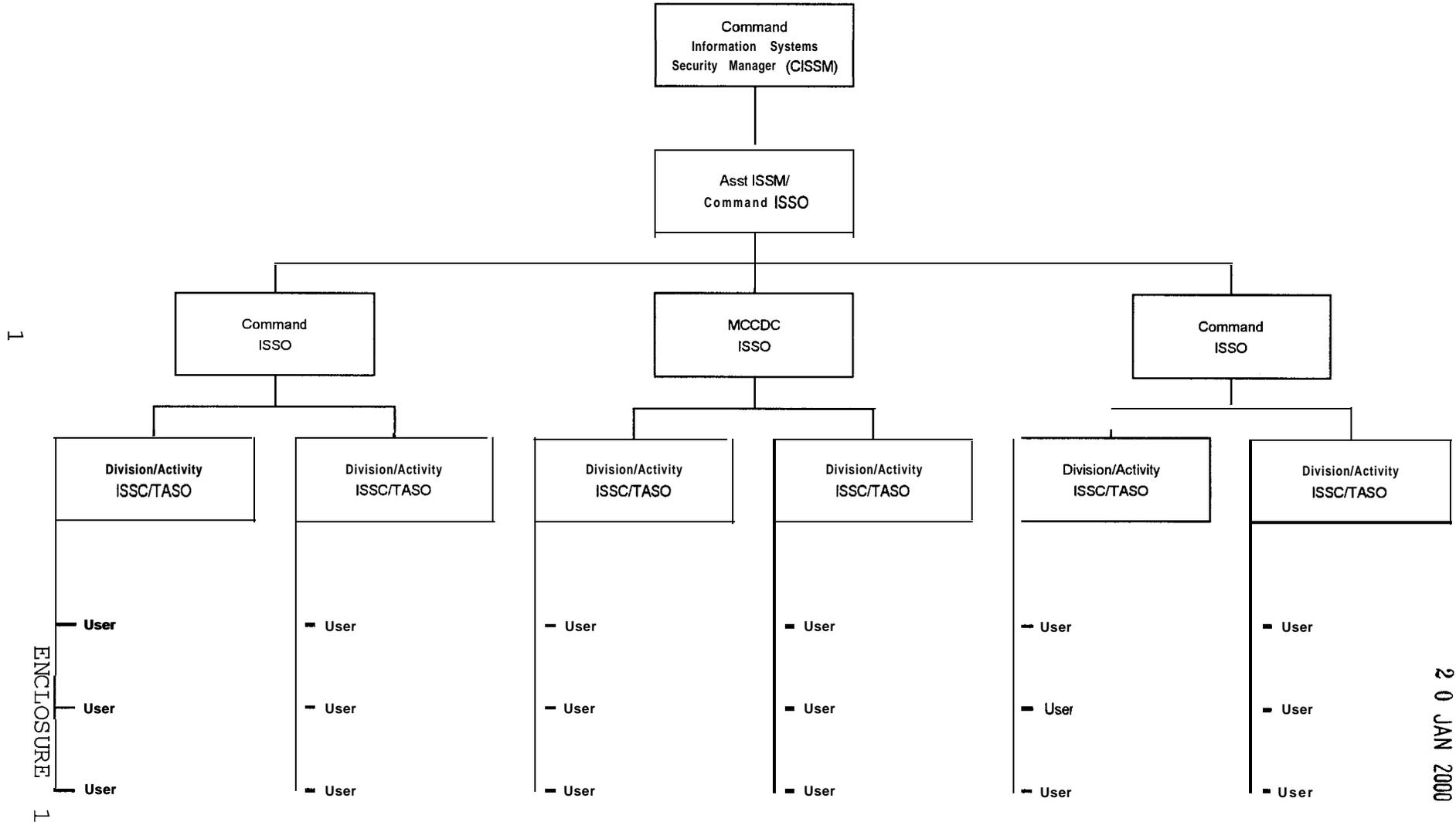
e. The Public Affairs Officer, in concert with the CISSM, will periodically publish information regarding this subject.



R. P. ROOK
Chief of Staff

DISTRIBUTION: INTERNET

Information Assurance, (IA) Administrative Framework



20 JAN 2000

NOTICE AND CONSENT LOG-ON BANNER

"THIS IS A DEPARTMENT OF DEFENSE (DOD) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."

(REFERENCE: DOD GENERAL COUNSEL MEMO, DATED 27 MAR 1997 APPLIES)

ENCLOSURE (2)