

COMSCINST 5235.1	COG CODE N6	DATE 11 AUG 1997
------------------	-------------	------------------



DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
WASHINGTON NAVY YARD BLDG 210
901 M STREET SE
WASHINGTON DC 20398-5540

COMSCINST 5235.1
N6
11 August 1997

COMSC INSTRUCTION 5235.1

Subj: WORLD WIDE WEB (WWW) AND INTERNET USE GUIDANCE

Ref: (a) COMSCINST 5230.1C Procedures for Requesting Command, Control, Communication and Computer (C4S) Services
(b) Military Sealift Command Common Operation Environment (COE) for Information Management

Encl: (1) Prohibited Use of Internet Services
(2) WWW Public Access Page Approval Process Flow Chart
(3) WWW Limited Access Page Approval Process Flow Chart

1. Purpose. To disseminate command policy for properly using, placing and maintaining information on the Internet.

2. Background. The Internet is a worldwide network of information resources intended for use as an interactive system for exchanging data. Through the Internet, Military Sealift Command (MSC) personnel have access to information from academic, scientific, governmental and commercial databases. The Internet also offers MSC the opportunity to provide information services to our customers via the WWW.

3. Policy

a. All requests for Internet User Accounts must be submitted to the local helpdesk. Local Helpdesks are listed in reference (a). The request must come from the user's supervisor and should include the following information:

- (1) User's full name
- (2) Office code
- (3) Phone number

11 August 1997

b. Only software authorized by Command, Control, Communications and Computer Systems (C4S) Director (N6) will be used by MSC personnel to access information resources on the Internet. Authorized software is listed in reference (b).

c. Files created by MSC personnel are considered Government records and will be treated as such. Files will not be transferred to mailing lists or remote hosts, unless it is required in connection with official business.

d. Use of the Internet is restricted to official business only (see enclosure (1)). No classified, Privacy Act protected, Freedom of Information Act or For Official Use Only (FOUO) information will be placed on the Internet where the general public can have access to the material.

e. MSC's homepage will be maintained by MSC Headquarters and will serve as the only front door to the public via the Internet. Field activities will be provided subpages for the placement of information unique to that field activity.

f. Public homepages will consist of information properly cleared for public release. Prior to being placed on the Internet, information must be reviewed and approved for public release. Enclosure (2) delineates the approval process. At the time of initial review, authorization to routinely update the data content should be requested. All initial pages must be reviewed and approved for public release by the following:

- (1) The originating Director
- (2) Command, Control, Communication and Computer Systems (C4S) Director (N6)
- (3) Counsel (N2)
- (4) Director, Public Affairs (N00P)

g. Limited Access homepages are non-public homepages. Prior to being placed on the Internet, information must be reviewed and approved for release. Enclosure (3) delineates the approval process.

4. Responsibilities

a. Command, Control, Communication and Computer Systems (C4S) Director (N6) is responsible for:

11 August 1997

(1) Managing and administering all hardware and software required to support Internet use. This includes WWW servers, any COMSC “homepage” and the loading of all data on the servers after release has been approved, as applicable (see reference (b)).

(2) Designating MSC’s Webmaster to serve as a focal point for routine WWW matters on a continuous basis.

(3) Establishing and enforcing security capabilities and protective measures including the development and operation of firewall technology.

(4) Providing style guidance for WWW page standardization (see reference (b)).

(5) Maintaining reference (b).

b. MSC Directors, Special Assistants, Program Managers and field activities are responsible for:

(1) Designating a point of contact (POC) to assist MSC’s Webmaster with procedural compliance.

(2) Submitting and keeping up-to-date information on sponsored web pages in accordance with MSC policy and style guidance

c. Counsel (N2) is responsible for:

(1) Designating a POC to assist MSC’s Webmaster with procedural compliance.

(2) Conducting and providing legal interpretations pertaining to information release with assistance of the Freedom of Information Act/Privacy Act (FOIA/PA) Coordinator, to ensure compliance with the FOIA Program.

(3) Reviewing and coordinating all web pages within 5 working days.

d. Director, Public Affairs (N00P) is responsible for:

(1) Designating a POC to assist MSC’s Webmaster with procedural compliance.

(2) Assuming and exercising clearance authority for release of public MSC information on the Public Access Web pages.

(3) Reviewing and coordinating all web pages within 5 working days.

COMSCINST 5235.1

11 August 1997

(4) Reviewing all submissions for compliance with MSC style standards.

5. Action. Directors/Special Assistants/Program Managers should give this policy the widest dissemination as possible.

Distribution:

COMSCINST 5000.19

List I (Case A, B, C)

11 August 1997

PROHIBITED USE OF INTERNET SERVICES

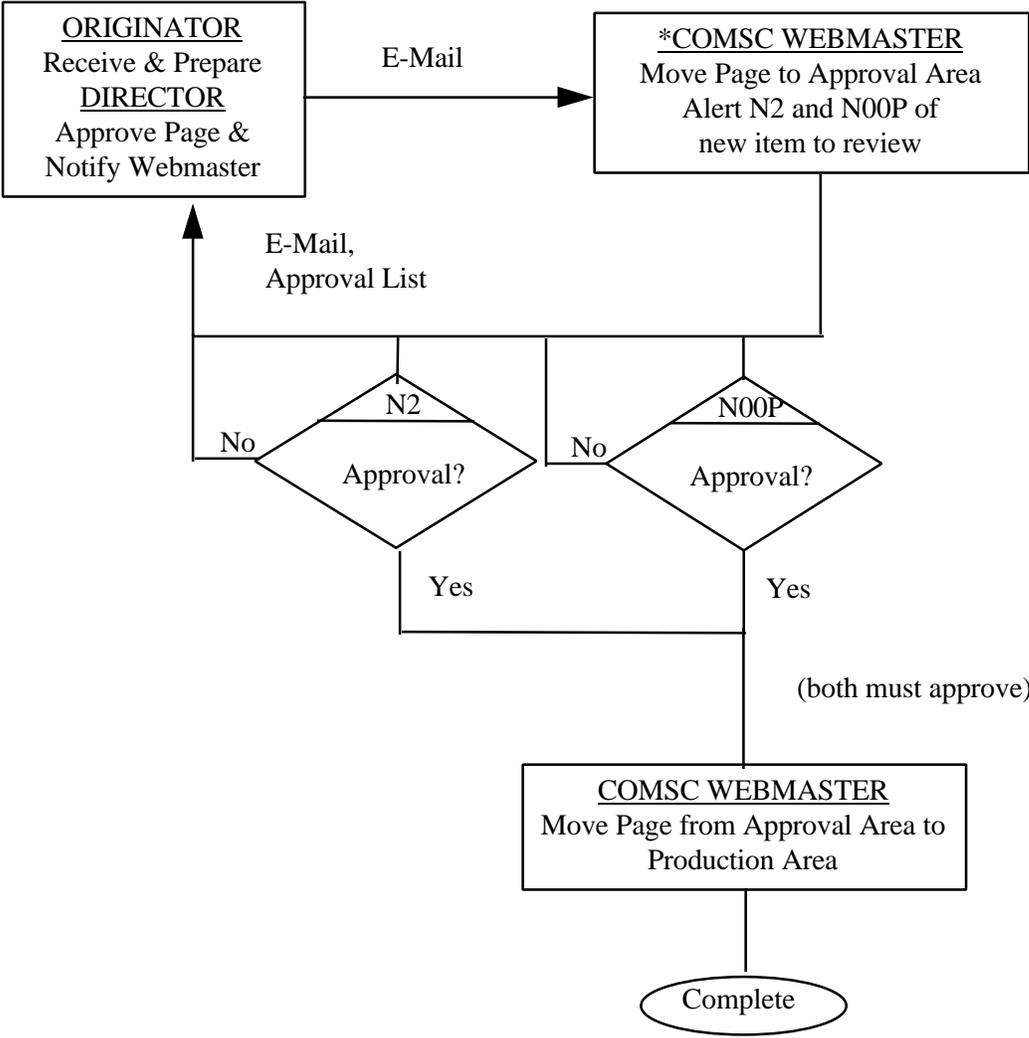
The use of Internet services in the following types of activities is specifically prohibited:

- **Illegal, fraudulent or malicious activities.**
- **Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organizations having no affiliation with USTRANSCOM or DoD.**
- **Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services and sales of personal property.**
- **Unauthorized fundraising or similar activities, whether for commercial, personal or charitable purposes. Official morale, welfare, recreation, officer and enlisted aid activities may be authorized.**
- **Accessing, storing, processing, displaying, transmitting or distributing offensive, sexually explicit or obscene material such as pornography and hate literature.**
- **Storing, processing or distributing classified, proprietary or other sensitive information on a computer or network not explicitly approved for such processing, storage or distribution.**
- **Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.**
- **Using another person's account or identity without his/her explicit permission, e.g., by forging e-mail, except when authorized by proper authority.**
- **Viewing, damaging or deleting files or communications belonging to others without permission or authorization by proper authority**
- **Attempting to circumvent or defeat security or auditing systems without prior authorization and other than as part of legitimate system testing or security research.**
- **Obtaining, installing, storing or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.**
- **Permitting any unauthorized person to access a U.S. Government-owned system.**

Violation of the listed prohibitions may result in adverse administrative or other disciplinary action being taken against the individual. Such actions may include proceedings pursuant to the Uniform Code of Military Justice, non-judicial punishments, personnel disciplinary actions and adverse comments/ratings on performance appraisals.

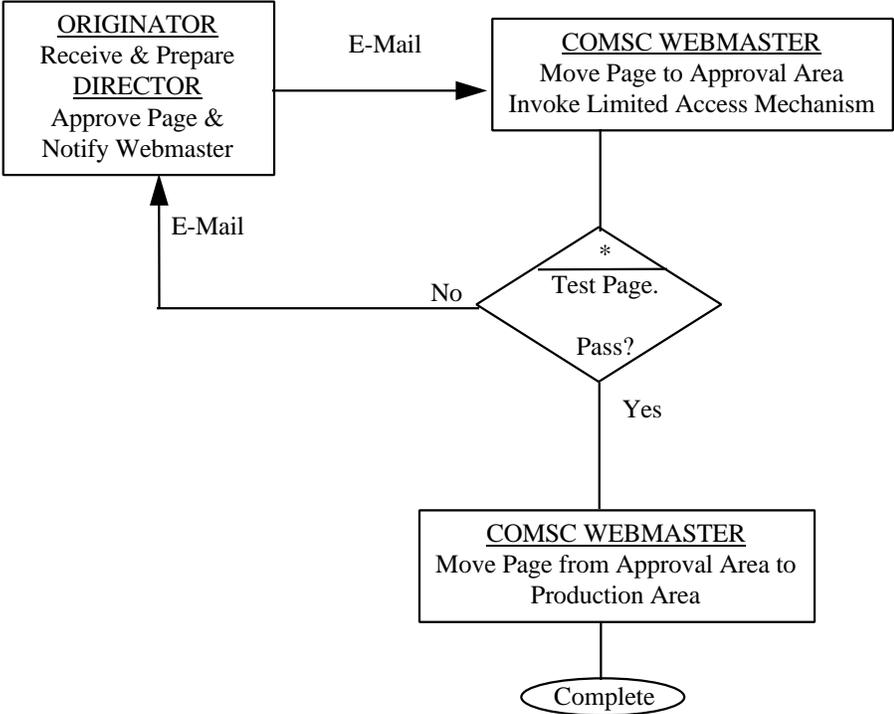
Enclosure (1)

WWW Public Access Page Approval Process



* Webmaster@smtpgw@msc.navy.mil

WWW Limited Access (Non- Public) Page Approval Process



* Page should be tested by a representative operational community (beta test).