



DEPARTMENT OF THE NAVY
NAVAL SUPPLY SYSTEMS COMMAND
5450 CARLISLE PIKE

PO BOX 2050 NAVSUPINST 2300.3B
MECHANICSBURG PA 17055-0791 SUP 069
8 May 2002

NAVSUP INSTRUCTION 2300.3B

Subj: USE OF COMMUNICATION SYSTEMS AND EQUIPMENT

Ref: (a) SECNAVINST 2305.11A
(b) DOD 5500.7-R

1. Purpose. To provide updated uniform guidance for the proper use of communication systems and equipment throughout the Naval Supply Systems Command (NAVSUP). This revision clarifies the authority of NAVSUP activity heads to ensure employee communications systems use is controlled and monitored. (R)

2. Cancellation. NAVSUPINST 2300.3A.

3. Background. References (a) and (b) prohibit Department of Navy (DON) civilian and military personnel from using Government services and equipment for other than official use and authorized purposes. Authorized purposes may include limited personal use of communication systems.

4. Definitions

a. Communication Systems and Equipment. Systems and equipment that transmit voice, data and/or video over a communication channel including, but not limited to, Government-owned telephones, facsimile machines, pagers, electronic mail, local and wide-area networks, the Internet and similar commercial systems when use is paid for by the Federal Government.

b. Official Use. Communication that is necessary for the conduct of official business. Official use includes emergency communication and communication that a Department of Defense (DOD) component determines is necessary in the interest of the Federal Government. Official use may include, when approved by theater commanders in the interest of morale and welfare, communication by military members and other DOD employees who are deployed for extended period away from home on official business.

c. Authorized Purposes. Brief communication made by DOD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes also include personal

0526-LD-101-4014

communication from the employee's usual workplace that is reasonably made while at the workplace.

d. Supervisor. For the purpose of authorizing personal use not covered by the blanket authorization contained in this instruction, or for revoking the blanket authorization, or parts thereof, the first supervisor who is a commissioned military officer or a civilian above GS/GM-11 in the chain of command or supervision of the DOD employee concerned.

5. Policy. Within NAVSUP the use of communication systems and equipment shall be for official use and authorized purposes only.

a. Blanket authorization is granted for the following personal uses of Government communication systems and equipment.

(1) Brief communication that is most reasonably made from the employee's normal workplace (such as checking in with spouse or minor children, scheduling doctor and auto or home repair appointments; brief Internet searches; e-mail directions to visiting relatives);

(2) Receipt of brief e-mail and facsimiles, as long as a comparable receipt would be acceptable via telephone, and the use is no more disruptive than a telephone call; and

(3) Conducting of job searches, and the preparation of resumes or employment applications in response to Federal Government downsizing.

b. The above authorization is subject to all of the following conditions:

(1) Whenever possible employees should limited personal communication, including Internet use, to authorized break periods or after-duty hours;

(2) Personal communication will be infrequent and short;

(3) Direct long distance charges or other fees must not accrue to the Government, i.e., employees must use toll-free numbers, charge any long distance communications to personal credit cards, or reimburse the Government for personal charges upon receipt of the official phone bill. (In general, long distance personal phone calls should be charged to the Government phone system only in emergency circumstances; personal credit cards or toll-free numbers should be used at all other times.)

(4) Communication that overburdens communication systems or equipment is prohibited;

(5) Except as specifically permitted herein communication to solicit or conduct business, advertising or other selling activities in support of a private business enterprise

or other non-federal organization, regardless of whether for profit, is not permitted;

(6) Communication must serve a legitimate public interest;

(7) Any other use that would reflect adversely on DOD or which is incompatible with public service (e.g., threatening or harassing phone calls or electronic messages; accessing, storing, processing, displaying, or distributing offensive, obscene, sexually explicit or pornographic material, or hate literature; unauthorized fundraising, gambling or similar activities; partisan political activity, political or religious lobbying or advocacy), or any other use that violates statute or regulation is not authorized;

(8) Frequent or systematic attempts to access prohibited (A) internet sites or telephone numbers is prohibited;

(9) Employees who access Federal Government communication systems and equipment or communication systems and equipment paid for by the Government, do so with the understanding that such use is neither secure nor anonymous, with no expectation of privacy. All use, regardless of whether official or authorized, is subject to monitoring. Furthermore, communication on Government communication systems and equipment may constitute Federal records within the meaning of the Federal Records Act and may be obtainable under the Freedom of Information Act;

(10) Any requests to use Federal Government communication systems that are not covered under this blanket authorization will be determined on a case-by-case basis by the supervisor and, except when clearly impracticable in remote locations, the organization's Ethics Counselor;

(11) Supervisors are responsible for ensuring the above limitations are adhered to;

(12) Supervisors may revoke this authorization, or parts thereof, for any perceived misuse; and

(13) Abuse of this privilege can serve as the basis of a disciplinary action up to and including removal from Federal Government service for civilian employees and punishment under the Uniform Code of Military Justice for military members.

6. Communications Monitoring and Control. NAVSUP activity heads will ensure the establishment of systematic programs to monitor communications systems use for compliance with the

(R)

aforementioned requirements. Such programs will be augmented with procedures and processes that both limit opportunities for unauthorized use and detect such use after its occurrence.

R) a. Activity heads will ensure that monitoring is conducted with a frequency sufficient to constitute a credible deterrent to unauthorized communications systems use. Where communications services such as electronic mail hub operations or Internet access are provided by external organizations, monitoring shall be ensured through the provisions of service level agreements, memorandums of understanding or contractual arrangements. Both the designation of content warranting detection and ensuring the systematic review of communications records, such as access logs and audit trails, are Command responsibilities that cannot be delegated or divested to any external service provider.

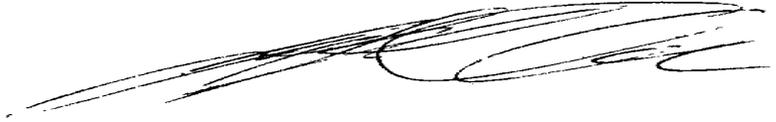
b. Controls will preclude access to Internet sites bearing content for which any degree of use would be inconsistent with the requirements of paragraph 5 of this instruction. Activities will also prohibit other communications use deemed excessive, unduly detrimental to productivity, or otherwise incompatible with activity mission requirements. Activity management is authorized to designate Internet sites to which access is prohibited, or conversely, to limit Internet access to only a specific range of predetermined sites meeting management approval. Access controls may also include precluding access to specific telephone numbers and imposing reasonable restrictions on the times of day or duration of any communications systems use.

R) c. Particular emphasis will be placed on prevention and detection of the uses prohibited in paragraph 5.b.7, using commercially available software or other means to continuously and systematically detect and block the transmission of messages, and access to Internet sites, bearing inappropriate content. Wherever feasible, electronic mail communications detected as including inappropriate content will be precluded from delivery to their intended recipient(s). Such nondelivery, however, will not diminish the responsibility of activity management to undertake whatever disciplinary action would have been appropriate had delivery occurred. Similarly, frequent or systematic attempts to access prohibited Internet sites or telephone numbers will warrant disciplinary action notwithstanding the fact that access has been unsuccessful.

7. Requests for Information. All media and public inquiries for information received through the Internet or any other communication system will be forwarded to the organization's Public Affairs Office and all Freedom of Information Act inquiries will be forwarded to the organization's Freedom of Information and Privacy Program Office.

NAVSUPINST 2300.3B
8 May 2002

8. Effective Date. This instruction is effective immediately. Addressees shall provide copies of internal disseminating guidance to NAVSUP (Code 06) within 30 days.



JEFFERY G. ORNER
Executive Director

Distribution:
FKM; X-32 (NAVSUP Offices and Directorates)

Copy to:
NAVSUP 35C (3 copies); 91; 93; 09I; NAVICP Mail Room M0852