



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-65
Phone: (202) 267-1798

COMDTINST 5375.1B
NOV 22 2004

COMMANDANT INSTRUCTION 5375.1B

Subj: LIMITED PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT

Ref: (a) Standards of Ethical Conduct, COMDTINST M5370.8 (series)
(b) Personal Use of Government Office Equipment, DHS MD Number 4600.1

1. PURPOSE. This Instruction refines the policy on *personal* use of government office equipment by all Coast Guard (CG) personnel in accordance with references (a) and (b). The use of government office equipment for official purposes is authorized and is not addressed by this Instruction.
2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, the Judge Advocate General, and special staff offices at Headquarters shall ensure compliance with the provisions of this Instruction. Internet release is authorized.
3. DIRECTIVES AFFECTED. Limited Personal Use of Government Office Equipment, COMDTINST 5375.1A, is hereby cancelled.
4. DISCUSSION. Since the inception of the original policy on limited personal use of government equipment, Information Technology (IT) systems and our IT infrastructure have become integral components of daily operational and business activities in the CG. While limited use of the IT infrastructure and the Internet by one person did not significantly impact official business, the aggregate use by many has negatively impacted the CG network.
5. AUTHORITY. Personal Use of Government Office Equipment, Department of Homeland Security (DHS) MD Number 4600.1; and, Article 92, Uniform Code of Military Justice (UCMJ).
6. DEFINITIONS.
 - a. Government Office Equipment: Office equipment and systems owned or leased by the government. This includes, but is not limited to: IT equipment, pagers, Internet services, email, library resources, telephones, facsimile machines, photocopiers, and office supplies.

DISTRIBUTION – SDL No. 142

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1	1	1	1	1		1	1		1	1	1	1	1	1		1		1					
B	1	8	10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	1	1		1	1	1	1	1	1	1	1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
E	1	1	1	1				1		1	1	1	1	1		1		1	1				1	1		
F																1	1	1								
G		1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

- b. Personal Use: Activity that is conducted for purposes other than accomplishing official business, educational, or otherwise authorized activity.
- c. Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes, but is not limited to, desktop computers, personal computers, laptops, handheld computers, Personal Digital Assistants (PDAs), related peripheral equipment, and software.
- d. Non-work Time: Any time CG personnel are not required to be performing assigned CG duties. Examples of non-work time include off-duty hours such as lunch periods, authorized breaks, before or after a workday, weekends or holidays, but only if your duty station would normally be available to you at such times.

7. POLICY.

- a. This Instruction is a lawful general order, punishable under Article 92 of the UCMJ. Violations of this Instruction may result in administrative and disciplinary action against military personnel. It is authority for taking adverse personnel actions against civilian employees. Violations of this Instruction may result in a person being held financially liable for the cost of prohibited or inappropriate use of government office equipment.
- b. Personnel must be authorized to use government office equipment for official Government business before it is available for limited personal use.
- c. Personal use of government office equipment is authorized for CG personnel only during non-work time, when such use:
 - (1) Involves minimal expense to the government.
 - (2) Does not reduce unit productivity or interfere with the mission or operations.
 - (3) Use of the Internet is limited to 30 minutes over a 24-hour period. Commands are authorized to approve additional personal use on a case-by-case basis.
- d. Managers and supervisors may further restrict personal use based on the needs of the command or office, or problems with unauthorized or inappropriate use.
- e. All CG personnel must comply with the requirements of this Instruction when telecommuting, in addition to existing policy regarding telecommuting.
- f. This Instruction shall be referenced in all CG Information User Agreements.
- g. Any unauthorized personal use incident (suspected or actual) must be reported to the local IT support staff and Information System Security Officer/Assistant (ISSO/ISSA), including accidental introduction of virus/worm, malicious software, accidental release of sensitive

information, or anything that compromises the confidentiality, integrity, availability, authentication, or non-repudiation of the CG enterprise IT infrastructure.

8. PROHIBITED USES.

- a. The following use of government office equipment is **prohibited at all times including non-work time** (exceptions are noted):

(1) Use of government office equipment to view, download, store, display, transmit, or copy any materials that are sexually explicit, or are predominantly sexually oriented. Sexually explicit or predominantly sexually oriented includes but is not limited to any material that depicts, in actual or simulated form, or explicitly describes, sexual content.

(2) Use of personal e-mail sites (e.g. Hotmail, AOL, MSN, Yahoo). These sites circumvent CG firewall / virus security measures.

Note: Personnel may utilize their “uscg.mil” e-mail account to send/receive a limited amount of personal e-mail while using a CG workstation. If using a “uscg.mil” account for personal reasons, a CG member or employee must not give the appearance that the United States Coast Guard endorses or sanctions that individual’s personal activities. If there is a potential for confusion, employees must provide an appropriate disclaimer, such as: “The content of this message does not reflect the official position of the United States, the Department of Homeland Security, or the Coast Guard.”

(3) Loading personal or unauthorized software onto a government computer or other government office equipment.

(4) Making configuration changes to a government computer system.

(5) Subscribing to or downloading streaming-data services (e.g., streaming video (MediaPlayer-type files), streaming audio (Internet radio stations), stock tickers (near real time stock market information), weather bug (live weather monitoring), news-flash tickers) or other automatic Internet services.

(6) Engaging in any fund raising activity, endorsing any company, service or product, or engaging in any political activity.

Note: Official fundraising activities are limited to Combined Federal Campaign and CG Mutual Assistance.

(7) Using government equipment as a staging ground or platform to gain unauthorized access to other systems.

(8) Using government office equipment for commercial purposes or to support a private or personal business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal or private business also precludes

employees using government office equipment to assist relatives, friends, or other persons in such activities.

- (9) Acquiring, reproducing, transmitting, distributing, or using any controlled information including computer software and data, protected by copyright, trademark, privacy laws or other proprietary data or material with other intellectual property rights beyond fair use, or export-controlled software or data.
 - (10) Deliberate introduction or failure to report accidental introduction of viruses, worms, or other malicious software.
 - (11) Accessing the following types of Internet sites (these are by way of example and not by limitation):
 - (a) Dating services web sites (e.g., match.com).
 - (b) Gaming or gambling oriented content.
 - (12) Accessing or using the following types of applications and associated web sites (including their use during a Remote Access Sessions (RAS)):
 - (a) Chat rooms for personal use (e.g. MSN Messenger, AIM, ICQ). An Internet chat session imposes significant risk to the network. There are many well-known vulnerabilities in the hacker community that exploit a chat session. The DHS and CG Portals will have a chat capability for government use.
 - (b) File sharing.
 - (c) Peer-to-Peer programs (e.g., Kazaa, Gnutella, Napster).
 - (d) Unauthorized outbound Remote Desktop Procedure (RDP) connections.
- b. Under no circumstances shall personally owned computers or personally owned IT equipment be connected to a CG network. This prohibits people from "jacking into" the CG network, for example, a visitor, contractor, or other employee connecting a personal computer into a network jack at a CG office or facility. This Paragraph does not include connecting via authorized CG remote access technologies (i.e., RAS).
 - c. As new threats arise that impact the Information Assurance (IA) posture of the CG, they will be published and the IA Program will implement appropriate protection strategies.

9. INAPPROPRIATE USES.

- a. The following personal use of government office equipment, not listed in paragraph 8 above, is **inappropriate** and may result in adverse administrative actions against an individual (exceptions are noted):
 - (1) Making personal long distance telephone calls.

Note: the exceptions are: in an emergency; a brief calls within the local commuting area to locations that can only be reached during working hours (e.g., car repair shop, doctor); and, a brief call home within the local commuting area (e.g., to arrange transportation, check on a sick child).

- (2) Creating, copying or transmitting any material or communication that is illegal or offensive to fellow employees or to the public, such as hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- (3) Creating, copying, or transmitting chain letters or other mass mailings (10 or more addressees), regardless of the subject matter.
- (4) Downloading, importing, copying or transmitting large Internet data files in excess of one Megabyte (i.e., digital pictures can easily exceed this file size).
- (5) Personal shopping sites (i.e., amazon.com, ebay.com).

Note: Afloat, deployed, and isolated unit Commanding Officers and Officers in Charge may authorize personal shopping on a case-by-case basis.

b. Inappropriate uses shall be amended as new threats arise that impact the IA posture of the CG.

10. LOCAL RESTRICTIONS. Commanding Officers and Officers in Charge may further reduce personal usage of government office equipment due to bandwidth restrictions as a result of increased operational tempo or degradation of network services (e.g., no attachments to email authorized).
11. DEPLOYED UNITS. Bandwidth is extremely limited for underway, forward deployed, and isolated units. Commands shall manage bandwidth, as an asset, to meet both mission requirements and to support unit morale. Commands are authorized to approve personal use on a case-by-case basis.
12. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this Instruction and have been determined to be not applicable.
13. FORMS/REPORTS. None.

T. H. COLLINS /s/
Admiral, U.S. Coast Guard
Commandant