DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF

MCCS-BIM

24 FEB 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-01, Use of Federal Government Communications Systems and Resources

1. REFERENCE. AR 25-1, Army Information Management, Chapter 6, 31 May 2002.

2. PURPOSE. The purpose of this memorandum is to provide reinforcement of the Army and local policy on use of Federal Government communications systems and resources.

3. SCOPE. This policy applies to all organizations and units located on or supported by Fort Sam Houston, Camp Bullis, and Camp Stanley, and that have connectivity to the installation network managed by the Information Technology Business Center (ITBC). This policy applies to both Government-owned and leased automation equipment.

4. BACKGROUND. The reference states, "The use of DOD and other Government telephone systems, e-mail and other systems (including the Internet) are limited to the conduct of official business or other authorized uses." The reference also states, "Users will not install new software packages, software upgrades, free software, freeware, shareware, etc., without the authorization of their systems administrator. Unauthorized software may contain harmful viruses or defects which can result in the loss of data or system failure."

5. POLICY. Current local policy does permit limited personal use of Government Internet and email resources. Such use must be before or after work, or during lunch or other authorized breaks during the workday. This permission does not extend to communications in support or furtherance of private business enterprises, or any other use that would reflect adversely on the Department of Defense. Examples of other uses that have an adverse impact include programs that use excessive bandwidth such as Napster, Gnutella, Weatherbug, and Realplayer. These and similar programs are not authorized for use on the installation network. In the recent past, users trying to do official business via the Fort Sam Houston network and Internet during normal duty hours (0715-1615) have experienced access speeds that are unacceptably slow because of the use of unauthorized applications.

6. It is, therefore, incumbent on all users to follow the Army and local policy. The reference also states "All information, including personal information placed on or sent over DOD computer systems may be monitored." The ITBC will continue monitoring the Fort Sam Houston network and will delete any unauthorized software applications. All incidents found will be sent through the applicable chain of command for appropriate action.

7. This policy will be reviewed 2 years from the implementation date.

8. The point of contact is Ms. Cynthia S. Helton, Director, ITBC, 221-5281, or email address Cynthia.helton@samhouston.army.mil.

DANIEL F. PERUGINI
Brigadier General, MC
Commanding

DISTRIBUTION:
A,B