

5-1. Information Transmission Economy and Systems Discipline Procedures.

Economy and discipline procedures include, as a minimum, the following:

a. A program and controls in place at all echelons to ensure that personnel are familiar with the types and purposes of available telecommunications and computing systems and can use them effectively.

b. Review and revalidation of all common-user Army telecommunications and computing systems, both Government and commercial, regardless of user. Dedicated information services and facilities are reviewed at least every two years by the appropriate DOIM. Review examines 800 numbers (purpose and traffic volume), and calling cards (assignment and how and from where used), as well as cellular phone and pagers (assignment, and how and when used).

c. Management and oversight of the use of long distance for telecommunications and computing systems, to include the Defense Information Systems Network (DISN) and cellular telephones.

d. A requirement for Telephone Control Officers to review and validate monthly bills for 800 service, pager service, cellular phone service, calling card usage; long distance DSN, Federal Telecommunications System (FTS) 2001, International Direct Distance Dialing (IDDD), and commercial calls; and local leased commercial service.

e. Collection for unofficial/personal toll calls placed on official telephones for telecommunications and computing systems. Commanders or the activity's equivalent have responsibility for the recovery of toll charges, as practical, for unofficial/unauthorized personal telephone calls placed on official telephones by personnel in their charge.

f. Privacy Act Provisions. Users of telecommunications and computing systems, including Internet access and the use of e-mail, are notified that their use of this equipment is subject to monitoring and recording. Use of government telecommunications and computing systems is made with the agreement that communications are not secure unless protected by authorized encryption devices and properly labeled for level of clearance authorized. System managers may employ monitoring tools to detect improper use of IT assets. Unauthorized or improper use of telecommunications and computing systems could result in disciplinary or financial penalties or other adverse actions.

g. Bandwidth Conservation. DoD is faced with serious restrictions on the amount of information that can be provided to our forces, particularly in remote areas of the world. While improvements to our communications networks are helping, they cannot keep pace with the demand. That is, we are "bandwidth constrained. The transmission of large non-operational documents and briefings sent over those networks may have serious operational impacts. DOIMs should ensure that users understand the impacts of bandwidth usage and develop procedures and encourage processes to reduce bandwidth demand. The amount and type of control on bandwidth usage should depend upon the organization's mission. Guidelines may consider the following:

(a) Use graphics sparingly in e-mail attachments. Avoid rich context pictures requiring large amounts of memory. Where possible, use text and graphics in black and white. Omit logos and seals on all but the title slide of a briefing.

(b) Use government provided e-mail services vice commercial web-based e-mail services, except where Government provided services are not available. Bandwidth overhead associated with the use of web-based e-mail is excessive and can constrict communication paths.

(c) Reduce lengthy e-mail document attachments and addressees, including the number of courtesy copies. Place documents on web servers whenever

possible. A Uniform Resource Locator (URL) can be provided indicating where the documents can be easily accessed via the Internet.

(d) Download large files from Web sites only when absolutely necessary and for official business. However, downloading from a Web site is preferable to sending lengthy files by e-mail to large lists of addressees. Install documents of high interest on the organization's Intranet or on the Internet.

(e) Compress large e-mail attachments to conserve bandwidth.

(f) Limit official subscriptions to newsgroups to those that support the organization's missions and functions. Reduce or eliminate individual personal subscriptions to newsgroups. Eliminate personal web services such as Pointcast.

(g) When using the "Reply" and "Reply to All" e-mail feature, avoid quoted replies/in-line replies (i.e., complete e-mail strings) to the maximum extent possible.

(h) Do not use the "Return Receipt" e-mail feature as a matter of routine. Use only on official e-mail when receipt must be positively verified (e.g., where the e-mail has a direct bearing on the mission).

(i) Install Intranets or shared network drive for sharing widely used documents.

h. Continuity of Operations Plans (COOP). Emergency and contingency requirements are generated by natural disasters, civil disturbances, exercise situations, mobilization, or war. All installation organizations have plans for the use of resources during any of these situations. One of the keys to effective mobilization will be the ability to provide command and control for the influx of troops into active duty. This may require a surge in information systems capability. See AR 380-19 for detailed information on COOP. See also AR 500-60, AR 500-70, DODD 3020.26, and DODI 3020.37.