5 FAM 500
TELECOMMUNICATIONS

5 FAM 510
TELECOMMUNICATIONS SERVICE AND EQUIPMENT

(CT:IM-100; 11-14-2008)
(Office of Origin: IRM/BPC/PRG)

5 FAM 511 GENERAL

(CT:IM-100; 11-14-2008)

a. Telecommunications refers to any technology, service, system, or other resource that provides or ensures transmission of electronic data and information. Telecommunication resources may be voice and data networks, telephones (wired and wireless), messaging and directory.

b. Telecommunications that is either all or part of a system must be considered an information technology (IT) system for all planning, acquisition, policy, security, and functional purposes. See 5 FAM 600.

c. All telecommunications equipment and services are for official U.S. Government use with only limited personal use by employees authorized as follows:

   (1) Employees may use Department of State unclassified office equipment (telephones, wireless technology, computers, printers, copiers, and facsimile machines) for limited personal use.

   (2) Limited personal use is authorized when it involves no additional expense (i.e., e-mail) or negligible expense to the government (e.g., electricity, ink, small amounts of paper, ordinary wear and tear) and is not excessive. Under no circumstances can U.S. Government resources be used to support the operation of a personal business operation.

   (3) Employees are to use personal time to perform tasks that are not official business. Employees must ensure that these personal tasks do not interfere with the conduct of official business, nor detract from the employee's performance in the workplace.

(4) Supervisors are authorized to, and should, limit personal use of U.S. Government equipment and resources if it becomes necessary because of cost, time away from official duties, degraded systems performance, or other business reasons. Limited personal use of government equipment and supplies is a privilege and not a right. Use may be restricted or revoked whenever appropriate in the interest of the government.

(5) Limited personal use does not apply to classified equipment or services. An exception is made for occasional electronic mail if the employee has no access to an unclassified e-mail system.

d. Users of telecommunications equipment and services must observe the procedures described in 5 FAH-2, Telecommunications Handbook.

e. All personnel performing Communications Security (COMSEC) accounting must observe the procedures described in 5 FAH-6, Communications Security Handbook (classified).

f. Department domestic organizations and posts abroad must address telecommunications outages and anticipated recovery actions in their electronic information processing continuity of operations plans or contingency plans (see 5 FAM 1064.2). Telecommunications outages can have a significant impact on the effective accomplishment of the Department's mission. See OMB Circular A-130, Management of Federal Information Resources and 12 FAM 622.3, Backup and Contingency Planning.

5 FAM 512 SCOPE AND AUTHORITIES

(CT:IM-100; 11-14-2008)

This chapter contains telecommunications policies for all users of the telecommunications systems identified and for specific personnel where indicated. The authorities established for this policy are as follows:

(1) 5 CFR 2635.704, Use of Government Property;

(2) 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch;

(3) 41 CFR subpart 101, Federal Property Management Regulations;

(4) Executive Order 12472 (June, 2006), Assignment of National Security and Emergency Preparedness Telecommunications Functions;

(5) National Security Decision Directive (NSDD) – 211, Diplomatic Telecommunications Service;

(6) OMB Circular A-130, Management of Federal Information

Resources, February 8, 1996;

(7) OMB Circular A-123, Management Accountability and Control, June 21, 1995;

(8) Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, Title III;

(9) National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 Security Requirements for Cryptographic Modules;

(10) NIST Special Publication (SP) 800-48 Wireless Network Security 802.11, Bluetooth and Handheld Devices;

(11) Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," November 18, 2002, Annex D, Part I, paragraph 2.1.5;

(12) Rehabilitation Act of 1973, as amended, Section 508 (29 U.S.C., section 794d);

(13) 36 Code of Federal Regulations (CFR) Part 1194, Architectural and Transportation of Barriers Compliance Board Electronic and Information Technology Accessibility Standards;

(14) Executive Order 13231, Critical Infrastructure Protection in the Information Age;

(15) Government Performance and Results Act (GPRA) of 1993, Public Law. 103-62;

(16) Paperwork Reduction Act of 1995, codified at 44 U.S.C., section 3501 et seq.; and

(17) OMB Memorandum 07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information, dated May 22, 2007.

5 FAM 513 DEFINITIONS

(CT:IM-100; 11-14-2008)

Automated Information System (AIS) is defined in 12 FAM 091.

Controlled Access Area (CAA) is defined in 12 FAH-6 H-021 (classified) and 12 FAM 091.

Communication Security (COMSEC) is defined in 12 FAM 091.

Contingency Plan is a plan maintained for emergency response, backup operations, and post-disaster recovery for an information system (IS), to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Information Technology (IT) is defined in 5 FAM 913.

Information Technology Change Control Board (IT CCB) is defined in 5 FAM 613.

Sensitive Compartmented Information Facilities (SCIF) is a accredited area, room, group of rooms, building, or installation where sensitive compartmented information may be stored, used, discussed and/or electronically processed.

Telephony is the science and practice of switching, transmitting, and receiving voice communications. Traditional telephone service was circuit switched and tightly controlled by telephone companies and long distance carriers. It now encompasses digital and wireless technologies and is merging with (IP) networks that are independent of the telephone companies and long distance carriers. See 5 FAH-2 H-600.

Telephony Circuitry is a system of electronic equipment that modulates, transmits, and receives voice and data signals via wire, wireless, or fiber optic light paths. See 5 FAH-2 H-610.

Voice Over Internet Protocol (VoIP) is a technology that allows telephone calls to be made over computer networks like the Internet. VoIP converts analog voice signals into digital data packets and supports real-time, two-way transmission of conversations using Internet Protocol (IP).

Wireless Tail Circuit is a local communication circuit that connects two or more separate compounds, buildings, or locations. Traditionally, tail circuits have utilized physical cabling, such as copper wire or fiber optic cable. Technology now supports the use of the wireless tail circuit that typically utilizes transceivers and antennae that facilitate a wireless signal, instead of physical cabling.

Wireless Technology permits the transfer of information between separate points without physical connection. Currently wireless technologies use Infra Red (IR), acoustic, radio frequency (RF), and optical but, as technology evolves, wireless technologies could include other methods of transmission.

5 FAM 514 THROUGH 519 UNASSIGNED