5 FAM 580
WIRELESS INFORMATION TECHNOLOGY (IT)

(CT:IM-92; 08-01-2007)
(Office of Origin: IRM/BPC/PRG)

5 FAM 581 PURPOSE AND SCOPE

(CT:IM-63; 06-06-2005)

a. This subchapter establishes **minimum** wireless IT policies and applies to wireless IT devices as defined in 5 FAM 583. These policies also apply to all Department of State personnel, contractors, and visitors (hereinafter referred to as users) who have access to Department facilities (domestic and abroad).

b. Telephones and pagers are addressed in 5 FAM 584 and 5 FAM 526. Television services are in 5 FAM 571. Acquisition of IT is covered in 5 FAM 900, Information Technology Acquisition; procurement of IT is in 5 FAM 920.

5 FAM 582 AUTHORITIES

(CT:IM-63; 06-06-2005)

The authorities for these policies are as follows:

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

(2) Office of Management and Budget (OMB) Circular A-130, Management of Information Resources;

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

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

(5) 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;

(6) Rehabilitation Act of 1973, as amended, Section 508 (29 U.S.C.

794d); and

(7) 36 Code of Federal Regulations (CFR) Part 1194, Architectural and Transportation Barriers Compliance Board Electronic and Information Technology Accessibility Standards.

5 FAM 583 DEFINITIONS

(CT:IM-63; 06-06-2005)

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

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

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

Information Technology Change Control Board (IT CCB) is defined in 5 FAH-5 H-512.

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

Synchronize in this subchapter refers to a two-way communication operation. This communication can be carried out wirelessly or through a physical connection between two wireless IT devices or between a wireless IT device and a computer.

Wireless IT is a system, device, transmitter, or receiver that detects, demodulates, and amplifies transmitted signals. It is telecommunications in which electromagnetic waves carry a signal or data over all or part of the communication circuit path without a physical connection. Wireless IT communication can be optical, radio frequency (RF), and audio. Mice, keyboards, networks, and routers can be types of wireless IT. Televisions, radios, headsets, microphones, remote controls, telephone, pagers and the like can also be considered wireless IT devices.

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. A wireless tail circuit typically utilizes transceivers and antennas that facilitate a wireless signal, instead of physical cabling.

5 FAM 584 TELEPHONE AND PAGER EQUIPMENT

5 FAM 584.1 Cellular Telephones

(TL:IM-47; 01-09-2004)

Cellular telephone policies are covered in 5 FAM 526.

5 FAM 584.2 Pagers

(TL:IM-47; 01-09-2004)

a. One-way pagers are receive-only pagers. Use of these pagers is permitted in all Department of State domestic facilities. Use of these pagers is permitted both inside and outside the Controlled Access Area (CAA) at posts abroad.

b. Two-way pagers have the ability to send and receive. This category includes voice pagers or any pagers that can send an acknowledgement back to the caller. These pagers may be brought into and used within Department of State domestic facilities but must be turned off when within ten feet from classified processing or discussions as they have active transmitters. This type of pager may not be brought into or used in a Sensitive Compartmented Information Facilities (SCIF) unless the senior official of the Intelligence Community (SOIC) has approved it for conduct of official duty (Director of Central Intelligence Directives (DCID) 6/9, Annex D, Part I, Paragraph 2.1.5). These type of pagers are permitted to be brought only into non-CAA spaces of buildings abroad and must be turned off when within ten feet from classified processing or discussions.

5 FAM 584.3 Ancillary Telephone Accessories

(TL:IM-47; 01-09-2004)

a. Use of radio frequency (RF) cordless or wireless telephones is not permitted in areas where classified information is discussed or processed, domestically, or abroad (see 12 FAH-6 H-531 x-5.1.i). They may be used domestically or abroad where classified information is neither processed nor discussed.

b. Entry of wireless telephones or handsets using Bluetooth technology is not permitted in any Department of State facility.

c. Use of cordless headsets is not permitted in close proximity to areas where classified information is discussed or processed, domestically, or in the CAA, abroad. A Security Engineering Officer (SEO) must perform a survey to determine the proximity issue, besides other security factors. The exceptions are headsets approved by DS/IST/CMP for people with special needs. HR/ER/WFP should be contacted to confirm there is a special need. They will coordinate the exception with DS/IST/ACD and

DS/IST/CMP (see 12 FAH-6 H-531 x-5.1.i).

5 FAM 585 PERSONALLY OWNED WIRELESS IT DEVICES

(CT:IM-63; 06-06-2005)

Personally owned wireless IT devices must not be connected to Department of State systems or networks. Abroad they must be left outside a CAA. Domestically, wireless IT devices must be turned off when within the 10-foot Spherical Zone of Control (SZOC) of:

(1) IT equipment processing classified national security information; and/or

(2) Areas where persons are conducting classified discussions.

5 FAM 586 DEPARTMENT-OWNED, -APPROVED AND -ISSUED WIRELESS IT DEVICES

5 FAM 586.1 Authorized Use of Department – Owned, -Approved and -Issued Wireless IT Devices

(CT:IM-63; 06-06-2005)

Department-owned, -approved and –issued wireless IT devices may be used to process sensitive but unclassified (SBU) information in Department facilities both domestically and abroad, provided these IT wireless devices are:

(1) IT CCB approved; and

(2) Properly configured with the IT CCB approved security software installed. Users must immediately notify the ISSO (refers to the designated ISSO, the alternate ISSO, or other assigned personnel who have been delegated specific ISSO authorities) and/or Regional Security Officer (RSO)/Post Security Officer (PSO) in the event of any significant security-related abnormal operation.

5 FAM 586.2 Department-Owned, -Approved, and -Issued Wireless IT Device Connection to non-State Owned Computers

(CT:IM-63; 06-06-2005)

Department–owned, -approved, and -issued wireless IT devices that synchronize or interface with the Department's OpenNet must not have simultaneous connection with any other systems via wired or wireless connection unless approved by the IT CCB.

5 FAM 586.3 Limitations on the Use of Department-Owned, -Approved, and –Issued Wireless IT Devices

(CT:IM-63; 06-06-2005)

a. Department-owned, -approved, and -issued wireless IT devices must use hardware and software approved by the IT CCB. (Contact the Enterprise Network Management Office (IRM/OPS/ENM) for information and guidance on the currently approved hardware and software standards.)

b. Only a cleared U.S. Citizen system administrator is authorized to reconfigure or update devices allowed in the CAA. In addition to cleared U.S. citizens, the Information Management Officer (IMO) may authorize Local Employed Staff (LES) or Foreign Service National (FSN) system administrators to configure and update devices that are restricted for use outside the CAA only. All devices must meet Department standards. (See 12 FAH-6 H-311.7, H-312.7, H-313.7, and H-314.7.)

c. Wireless IT devices must neither process nor store classified information. These devices also must not connect to a classified AIS.

5 FAM 587 GUIDANCE FOR USE OF DEPARTMENT-OWNED, -APPROVED, AND –ISSUED WIRELESS IT DEVICES

5 FAM 587.1 Domestic Use of Department-Owned, -Approved, And -Issued Wireless IT Devices

(CT:IM-63; 06-06-2005)

a. Bureau Executive Directors must approve the distribution and use of Department-owned, IT CCB-approved, wireless IT devices within their Bureaus.

b. Executive Directors have the overall responsibility to ensure that all Department-owned, -approved, and -issued wireless IT devices are maintained in a property inventory.

c. An ISSO must brief wireless IT device users on appropriate security procedures for handling and use prior to issuing a Department-owned, -approved, and -issued wireless IT device. The ISSO must maintain a written record and signed user acknowledgement of the briefing.

d. Users must immediately report the loss or theft of a wireless IT device. A formal written report must be submitted to the property manager, the bureau ISSO, and the Unit Security Officer (USO). Users must also immediately notify the ISSO in the event of any significant security-related abnormal operation.

e. Department-owned, -approved, and -issued wireless IT devices must not be operated inside a 10-foot SZOC of:

   (1) IT equipment processing classified national security information; and/or

   (2) Areas where persons are conducting classified discussions.

5 FAM 587.2 Use Of Department-Owned, -Approved, and -Issued Wireless IT Devices Abroad

(CT:IM-63; 06-06-2005)

a. The Management Officer (MO) must approve the distribution and use of Department-owned, IT CCB-approved, wireless IT devices at post.

b. The MO has overall responsibility to ensure that all Department-owned, -approved, and -issued wireless IT devices are maintained in accordance with post's property inventory procedures, including formal receipt as required.

c. The ISSO must brief wireless IT device users on appropriate security procedures for handling and use prior to issuing a Department-owned, -approved, and -issued wireless IT device. The ISSO must maintain a written record and signed user acknowledgement of the briefing.

d. The user must immediately notify the ISSO, RSO/PSO, and property manager in writing of the loss or theft of a wireless IT device. A formal written report must be submitted to the property manager, the bureau ISSO, and the RSO/PSO. Users must also immediately notify the ISSO or RSO/PSO in the event of any significant security-related abnormal operation.

e. Department-owned, -approved, and -issued wireless IT devices must not be allowed in the CAA unless authorized under Department standards. (See 12 FAH-6 H- 311.7, H-312.7, H-313.7, and H-314.7.)

5 FAM 588 DEPARTMENT-OWNED AND - APPROVED WIRELESS LOCAL AND WIDE AREA NETWORK AND EQUIPMENT

5 FAM 588.1 Domestic Use of Department –Owned and - Approved Wireless Networks and Equipment

(CT:IM-63; 06-06-2005)

Domestic users of wireless IT network components must use IT CCB-approved wireless network components and network devices. They must not be connected to or used with any classified equipment or networks.

5 FAM 588.2 Use of Department-Owned and - Approved Wireless Networks and Equipment Abroad

(CT:IM-63; 06-06-2005)

a. Users of wireless IT network components abroad must use IT CCB-approved wireless network components and network devices. They must not be connected to or used with any classified equipment or networks.

b. Wireless network devices must not be installed inside CAA spaces.

c. Posts must coordinate the configuration, installation and operations with their Regional Information Management Center (RIMC), the Regional Computer Security Officer (RCSO), the Office of Security Technology (DS/C/ST), and the Office of Computer Security (DS/SI/CS) to ensure installation security requirements are met and proper wireless network operations are maintained.

5 FAM 588.3 Use of Department-Owned And - Approved Wireless Tail Circuits And Other Wireless Circuits

(CT:IM-63; 06-06-2005)

a. Wireless tail circuits may be used when physical cable infrastructure is not available or when business requirements dictate. Wireless tail circuits may also be implemented as temporary backup systems to traditional wired tail circuits.

b. When a backup wireless tail circuit is not in use, power to the circuit equipment, such as the wireless transceiver, must be disconnected.

Additionally, backup wireless tail circuits must only be powered and operated while a primary wired tail circuit is not functional and/or being serviced.

c. To transit data over a wireless infrastructure, you must use National Institute of Standards and Technology (NIST) accredited and National Security Agency (NSA) approved products to encrypt the data. In addition, the IT CCB must approve the use of all encryption devices used on the SBU network.

d. Wireless tail circuit requests must be made through the IRM InfoCenter.

5 FAM 589 ACCESSIBILITY REQUIREMENTS FOR PEOPLE WITH DISABILITIES

(CT:IM-63; 06-06-2005)

a. Medical devices are exempt from the policies in 5 FAM 586 through 5 FAM 589. Medical devices include, but are not limited to, hearing aids, pacemakers, or other implanted medical devices.

b. The Countermeasures Program Division (DS/ST/CMP) must approve all wireless accessibility devices for employees with disabilities to be used in a CAA abroad. All reasonable effort will be made to provide wireless IT devices to employees with disabilities that both:

(1) Do not pose a risk to the discussion or processing of classified information; and

(2) Are compliant with Section 508 of the Rehabilitation Act of 1973 and relevant implementing regulations (36 CFR 1194).

c. IRM/BPC/CST/BC/SAS (IMPACT office) must be contacted regarding Section 508 questions. The Work/Life Program Division (HR/ER/WLP) must be contacted to confirm that a special need exists and answer questions regarding reasonable accommodation for employees with disabilities. Discussion or approval of any waiver/exception to DS requirements must be coordinated with DS/SI/CS and DS/ST/CMP.