# 5 FAM 870
# NETWORKS

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

## 5 FAM 871  ENTERPRISE NETWORKS

*(TL:IM-50;  05-04-2004)*

The Department currently has two enterprise networks:  classified (ClassNet) and unclassified (OpenNet).  Only Department issued or approved systems are authorized to connect to Department networks.

## 5 FAM 872  CLASSNET

*(CT:IM-68;  10-06-2005)*

a. The Department's ClassNet provides a Secret data network and supports internal Department Secret e-mail and access to the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNET). ClassNet also provides Cable Xpress, which is currently the Department's sole telegram processing program.

b. All ClassNet changes (i.e., baseline and modifications) must be submitted to the Local Change Control Board (CCB) for initial review and evaluation, and forwarded to the Information Technology Change Control Board (IT CCB) for final review, evaluation and approval.

c. Users must not load Classified information onto unclassified systems, and any information exchange between classified and unclassified systems may only occur following established Department guidelines, developed by Diplomatic Security (DS) or with a recommended waiver by DS and approved by the Chief Information Security Officer (CISO).

d. Passwords must be properly protected from unauthorized disclosure.

e. Users have no expectation of privacy when using Department systems. Equipment is closely monitored at all times for user actions and data classification.

f. Official portable computers must not be connected to ClassNet systems without explicit approval of the bureau or post Information Systems

Security Officer. This equipment must have all Department-required software patches applied and must have current anti-virus software and definitions installed. Personally owned computers must not be connected to ClassNet under any circumstances and must not be used within Control Access Areas (CAAs) at any time. (See 12 FAM 625.)

# 5 FAM 873 OPENNET/OPENNET PLUS

*(CT:IM-68; 10-06-2005)*

a. OpenNet is the Sensitive but Unclassified (SBU) network in the Department. It provides standard desktop applications such as word processing, e-mail, and Internet web browsing and supports a battery of custom Department software solutions and database management systems.

b. All OpenNet/OpenNet Plus changes (i.e., baseline and modifications) must be submitted to the Local CCB for initial review and evaluation. The change may be approved by the Local CCB or forwarded to the IT CCB for final review, evaluation and approval, per the IT CCB SOP guidelines.

c. Users sending personal e-mail out to the Internet should make it clear, in an appropriate place in the message, that his or her e-mail is not being used for official business. (See 12 FAM 642.4-3 Pre-Logon Warning Message for disclaimer.)

d. Users must not exchange information between classified and SBU systems.

e. Passwords must be properly protected from unauthorized disclosure.

f. Users have no expectation of privacy when using Department systems. Equipment is closely monitored at all times for user actions and data classification.

g. Official portable computers must not be connected to OpenNet systems without explicit approval of the bureau or post Information System Security Officer (ISSO). This equipment must have all Department-required software patches applied and must have current anti-virus software and definitions installed. Personally owned computers must not be connected to OpenNet under any circumstances and must not be used within Control Access Areas (CAAs) at any time. (See 12 FAM 625.)

h. For specific guidance on transport and use of portable computers at post, contact DS/IST/ACD.

# 5 FAM 874 CONNECTIONS TO THE INTERNET AND USE OF DEDICATED INTERNET NETWORKS (DINS)

## 5 FAM 874.1 CONNECTIONS TO THE INTERNET

*(CT:IM-56; 01-24-2005)*

a. All bureaus and posts having access to OpenNet are required to establish Internet connectivity through OpenNet Plus. If OpenNet service is available to the bureau/post, the Department will no longer fund or approve Dedicated Internet Network (DIN) service unless the bureau or post has a valid waiver to implement a DIN.

b. A post may have a contract with an Internet Service Provicer (ISP) to provide bandwidth for contingency and VNet (also know as Virtual Private Network (VPN)) provided and managed by IRM/OPS/ENM/ND. This is to provide the post with an alternate route for connectivity back to the Open Net infrastructure and does not require a waiver.

c. Information Resource Center (IRC) public access terminals have been granted a waiver from this policy; i.e., ODI (Overseas Dedicated Internet) LANs may continue to provide Internet access and other Public Diplomacy services to the public. Local networks used as test, development, web hosting, and research environments may also connect locally to the Internet, but can only do so after receiving a waiver (see 5 FAM 874.2). These Local Area Networks (LANs) are not to be linked to OpenNet Plus or used by employees to carry out Department business transactions. Bureau/post must terminate all unauthorized use of ODI LANs no later than 90 days after OpenNet Plus is implemented at the bureau/post.

d. The Department realizes that there may be exceptions to the requirement for accessing the Internet via the OpenNet. Posts and bureaus may request a waiver to this policy. The IT CCB will review such requests on a case-by-case basis. See 5 FAM 874.2 Requesting a Waiver to the Internet Connection Policy.

## 5 FAM 874.2 REQUESTING A WAIVER TO THE INTERNET CONNECTION POLICY

*(TL:IM-50; 05-04-2004)*

a. A Bureau/post requesting authorized continued use of a Dedicated Internet Network (DIN) connection must submit the DIN access waiver

request. All DIN solutions must comply with the Department's standards and FAM guidance. Provide the following information when submitting the waiver request:

(1) Post or bureau name;

(2) Post or bureau point of contact, e-mail address, and telephone number;

(3) Location serviced by DIN;

(4) Type of Internet access service (DSL, dial-up, other);

(5) Configuration details (number of connections, users, rooms to be served);

(6) Purpose of the service;

(7) Reason requirement cannot be satisfied through OpenNet Plus (for example: Protocol is not available through OpenNet Plus—website not accessible);

(8) What post/bureau is doing to reduce risks (i.e. firewalls, virus protection);

(9) Projected costs; and

(10) Timeframe of exception.

d. Submit DIN Access Waiver Requests by e-mail to "IT CCB Management" or by telegram or memorandum to the IT CCB Change Manager, IRM/OPS/ENM/NLM/ECM. The IT CCB Change Manager will conduct an abbreviated review with relevant IT CCB primary review authorities and will ensure the request appears on the next IT CCB meeting agenda for consideration and decision.

e. If a request for a waiver is denied, the bureau/post may send an appeal to the Chief Information Officer for final decision.

f. If a bureau/post's network is connected to the Internet outside of OpenNet Plus and without the signed DIN waiver, the bureau/post is in conflict with security guidelines, such as those in 12 FAM 600. If unauthorized Internet connections are detected, the responsible office will be instructed to disconnect them.

# 5 FAM 875 THROUGH 879 UNASSIGNED