5 FAM 870
NETWORKS

(CT:IM-116; 05-19-2011)
(Office of Origin: IRM/BMP/GRP/GP)

5 FAM 871 ENTERPRISE NETWORKS

(CT:IM-105; 05-14-2009)

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

5 FAM 871.1 ClassNet

(CT:IM-109; 05-05-2010)

a. The Department's ClassNet provides an internal network for e-mail and other processing of information up to the SECRET level and provides access to the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNET).

b. Submit all ClassNet changes (i.e., baseline and modifications) to the Information Technology Change Control Board (ITCCB) for review, evaluation, and decision.

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

d. Users have no expectation of privacy when using Department systems. The system is monitored at all times for user actions and data classification.

e. Only Department-owned and IT CCB-approved hardware (including removable media) and software are permitted to be installed or used on classified Department automated information systems (AISs). Computers connected to ClassNet must have all Department-required software patches applied and must have current anti-virus software and definitions installed. Additionally, portable computers must not be connected to ClassNet systems without explicit approval of the bureau or post information systems security officer. See 12 FAM 630 for additional security requirements.

5 FAM 871.2 OpenNet

(CT:IM-109; 05-05-2010)

a. OpenNet is the Sensitive but Unclassified (SBU) network in the Department. It provides access to 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. Submit all OpenNet changes (i.e., baseline and modifications) to the local CCB for initial review and evaluation. The change may be approved by the local CCB or sent via unclassified e-mail to their voting sponsor and ITCCB management for final review, evaluation, and decision, per ITCCB SOP guidelines. See 5 FAM 862 for more information regarding local CCB processes and responsibilities.

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.

d. Users must not load classified information onto unclassified or SBU systems, and any information exchange between classified and unclassified or SBU 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).

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

f. Only Department-owned and -ITCCB or local -CCB-approved hardware (including removable media) and software are permitted to be installed or used on SBU Department AISs. (All operating system software must be IT CCB-approved.) Computers connected to the OpenNet must have all Department-required software patches applied and must have current anti-virus software and definitions installed. Additionally, portable computers must not be connected to OpenNet systems without explicit approval of the bureau or post information system security officer (ISSO). See 12 FAM 620 for additional security requirements.

g. For specific guidance on transport and use of portable computers at post, contact the Office of Computer Security (DS/SI/CS).

5 FAM 872 CONNECTIONS TO THE INTERNET

AND USE OF DEDICATED INTERNET NETWORKS (DINS)

5 FAM 872.1 Connections to the Internet

(CT:IM-116; 05-19-2011)

a. *The use of a Dedicated Internet Network (DIN) is to provide services not currently provided on OpenNet Plus (ONP).* 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 registered their DIN.

b. A post may have a contract with an Internet service provider (ISP) to provide bandwidth for contingency and VNet (also known 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 OpenNet infrastructure and does not require registration.

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 registration (see 5 FAM 872.2). 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. Approved DINS may be used for a variety of applications. However, they are not to be:

(1) Linked to OpenNet or used by employees to carry out Department business transactions,

(2) Used to transmit Sensitive but Unclassified (SBU) data, or;

(3) Used to transmit Personally Identifiable Information (PII).

(4) Refer to the IT CCB SharePoint site *for Additional information on ODI/DIN use.*

e. The Department realizes that there may be exceptions to the requirement for accessing the Internet via the OpenNet. Posts and bureaus must register their DIN. There are no exceptions to this policy. The IT CCB will review these registrations as they are submitted. See 5 FAM 872.2, DIN Registration Policy.

5 FAM 872.2 DIN Waiver Registration Policy

(CT:IM-116; 05-19-2011)

a. A bureau or post requesting authorized continued use of a Dedicated Internet Network (DIN) connection must register. All DIN solutions must comply with the Department's standards and FAM guidance. Provide the following information when registering the waiver:

(1) Title/registration name;

(2) Request date;

(3) Post or bureau name;

(4) ISSO;

(5) Point of contact;

(6) Purpose of service;

(7) Justification;

(8) Type of network;

(9) Firewall type;

(10) Number of users;

(11) Number of workstations;

(12) Number of servers;

(13) Expiration date;

(14) Target audiences;

(15) ITAB Registration ID#; and

(16) Connection cost.

b. Register DIN Access by completing the required fields on the IT CCB DIN Registration page *(the link takes you to the DIN Approvals page—select the "New" button)*. The IT CCB Change Manager will review the registration to ensure compliance with appropriate requirements.

c. Any unregistered DIN, with the exception of an IRC, is unauthorized and must be either immediately registered or else disconnected.

5 FAM 873 THROUGH 879 UNASSIGNED