5 FAM 840
MANAGING SYSTEMS

(CT:IM-89;   05-30-2007)
(Office of Origin: IRM/APR/RG)

5 FAM 841 SYSTEMS AUTHORIZATION PROCESS

(CT:IM-89;   05-30-2007)

a. In accordance with OMB A-130, the Department is required to make a security determination, called authorization, to permit placing IT systems into operation. In order for officials to make fully advised risk-based decisions, they must conduct a security evaluation known as certification of the IT system.

b. All IT systems must complete the systems authorization process before becoming operational. *(See 5 FAM 1060 and 5 FAM 611)*.

5 FAM 842 INFORMATION TECHNOLOGY SECURITY PLANS

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

a. The Federal Information Security Management Act (FISMA) 2002 and OMB Circular A-130 require all major applications and support systems to have a security plan. The system security plan provides all the information necessary to secure an IT system throughout the system's lifecycle.

b. See Information Assurance for the available tool.

5 FAM 843 INFORMATION QUALITY

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

OMB requires each agency to establish guidelines on ensuring the integrity of the information it maintains. Department guidelines state that each post and bureau is responsible and accountable for the integrity of information

maintained on its IT systems. Information Management Officers(IMO)/ Information Systems Officers(ISO)/System Owners must carry out these responsibilities. See Department's Quality Guidelines.

5 FAM 844 STORING, HANDLING, AND DESTROYING MEDIA

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

To protect information from loss, damage, or compromise, the ISO/system administrators and Information Systems Security Officer (ISSO) must verify destruction of media. For further guidance see 12 FAM 622.1-7 and 12 FAM 622.1-11 for unclassified/SBU media and 12 FAM 632.1-6 and 12 FAM 632.1-9 for classified media.

5 FAM 845 SECURITY AWARENESS, TRAINING, AND EDUCATION

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

a. The Department is required by the Federal Information Security Act (FISMA) 2002 to conduct computer security training to ensure the confidentiality, integrity, and availability of its computer-based information.

b. DS/T/TPS/SECD implements the Department's Information Assurance (IA) role-based training program. IRM/IA has responsibility for ensuring that Department's IA training program complies with federal guidelines. For courses offered, see DS Training and Information Assurance.

c. Annual IT security awareness briefings for users are initiated, developed, and provided by DS/IS/CSD or others authorized by the CISO to conduct the briefing.

d. 12 FAM 600 requires the ISSOs, IMOs, and System Administrators to ensure that all users receive appropriate security training. COTRs/ Contracting Officer Representatives (CORs) are responsible for their contract employees, and must ensure that all contracted employees receive appropriate systems security training before accessing any bureau or post system.

5 FAM 846 ANTI-VIRUS

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

All IMOs/ISOs/System Administrators for classified and unclassified systems are required to implement virus protection and detection programs for all systems connected to the Department's network, per 12 FAM 643.2-9 Virus Prevention.

5 FAM 847 FIREWALLS

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

a. The Department uses firewall technology to provide protection for network resources at all points where the internal networks connect with non-Department networks.

b. The Department's Firewall Advisory Board, chaired by IRM/OPS/MSO/EML, ensures consistency of protection worldwide by establishing a baseline configuration for each of the Department firewalls.

c. IMOs/ISOs/System Administrators must comply with all guidance provided by the Firewall Advisory Board.

5 FAM 848 REMOTE ACCESS

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

Domestically, the Department is able to provide employees with Secure dial-up access to Department resources by using Secure Domestic Dial-in (SDDI) to access their Sensitive but Unclassified (SBU) e-mail accounts and the Department's Intranet from locations outside of their normal office. Information on SAFENET is found on the InfoCenter Web site Secure Dial-up.

5 FAM 849 AUDIT TRAILS

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

With guidance from the Regional Security Officer (RSO)/Post Security Officer (PSO) and Regional Computer Security Officer (RCSO) and 12 FAM 600, a post's ISSO is responsible for coordinating with IMOs/ISOs/System Administrators to monitor, investigate, log, and report system events and activities resulting from unauthorized access and modifications of sensitive critical files. See 12 FAM 600 for further guidance.