

5 FAM 850 CONTINUITY OF OPERATIONS AND CONTINGENCY PLANNING FOR INFORMATION SYSTEMS

(CT:IM-97; 09-24-2008)
(Office of Origin: IRM/APR/RG)

5 FAM 851 REQUIREMENTS

(CT:IM-97; 09-24-2008)

- a. In accordance with OMB A-130, every information system in the Department must have a contingency plan. This plan must be developed, documented, and tested *each year* for each general support system and major application.
- b. System Administrators may download an appropriate contingency planning tool from the IRM/IA web page. *For additional information on contingency planning see 12 FAM 622.3 and 12 FAM 632.3, along with NIST SP 800-34. The contact at the Office of Emergency Management (OEM) for (COOP) is Mr. Art Mock at 202-776-8603, Fax 202-457-0337.*

5 FAM 852 BACKUPS

(CT:IM-97; 09-24-2008)

- a. Regardless of the size of the system, system and data files must be backed up regularly (at least once per week). The IMO/ISO/System Administrator has responsibility to:
 - (1) Establish a method and time for backups and adhere to the schedules;
 - (2) Determine which files are to be backed up, and when and how they will do it;
 - (3) Decide when to back up based on the local operational environment; and
 - (4) Notify users of backup schedules.
- b. Copies of backup tapes or disks must be stored in a safe place off-

site.

- c. Users should back up critical files on their own PCs on an established schedule as a precaution.
- d. See 12 FAM 622.3-1 Backup or 12 FAM 632.3-1 Backup for more information.

5 FAM 853 THROUGH 859 UNASSIGNED