

special access programs, and the mechanisms for monitoring such programs?

(ix) What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

(x) What are the requirements for oversight of the security classification program, including agency self-inspections?

(d) *Refresher security education and training.* Agencies shall provide refresher training to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during agency self-inspections. When other methods are impractical, agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

(e) *Termination briefings.* Each agency shall ensure that each employee granted access to classified information who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn must receive such a briefing. At a minimum, termination briefings must impress upon each employee: The continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

(f) *Other security education and training.* Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include:

(1) Practices applicable to U.S. officials traveling overseas;

(2) Procedures for protecting classified information processed and stored in automated information systems;

(3) Methods for dealing with uncleared personnel who work in proximity to classified information;

(4) Responsibilities of personnel serving as couriers of classified information; and

(5) Security requirements that govern participation in international programs.

Subpart E—Declassification

§ 2001.50 Definition [3.1].

A *file series* is a body of related records created or maintained by an agency, activity, office or individual. The records may be related by subject, topic, form, function, or filing scheme. An agency, activity, office, or individual may create or maintain several different file series, each serving a different function. Examples may include a subject file, alphabetical name index, chronological file, or a record set of agency publications. File series frequently correspond to items on a NARA-approved agency records schedule. Some very large series may contain several identifiable sub-series, and it may be appropriate to treat sub-series as discrete series for the purposes of the Order.

§ 2001.51 Automatic declassification [3.4].

(a) *General.* All departments and agencies that have original classification authority, or previously had original classification authority, and maintain records appraised as having permanent historical value that contain information classified by that agency shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in carrying out an automatic declassification program involving accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist of the United States. The Archivist will not declassify information created by another agency without the prior consent of that agency.