

(2) Elements of classifying and declassifying information.

(i) What is classified information and why is it important to protect it?

(ii) What are the levels of classified information and the damage criteria associated with each level?

(iii) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(iv) What are the general requirements for declassifying information?

(v) What are the procedures for challenging the classification status of information?

(3) Elements of safeguarding.

(i) What are the proper procedures for safeguarding classified information?

(ii) What constitutes an unauthorized disclosure and what are the criminal, civil, and administrative penalties associated with these disclosures?

(iii) What are the general conditions and restrictions for access to classified information?

(iv) What should an individual do when he or she believes safeguarding standards may have been violated?

(c) *Specialized security education and training.* Original classification authorities, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date. Coverage considerations should include:

(1) Original Classification Authorities.

(i) What is the difference between original and derivative classification?

(ii) Who can classify information originally?

(iii) What are the standards that a designated classifier must meet to classify information?

(iv) What discretion does the Original Classification Authority have in classifying information, for example, foreign government information.

(v) What is the process for determining duration of classification?

(vi) What are the prohibitions and limitations on classifying information?

(vii) What are the basic markings that must appear on classified information?

(viii) What are the general standards and procedures for declassification?

(2) Declassification authorities other than original classification authorities.

(i) What are the standards, methods and procedures for declassifying information under Executive Order 12958, as amended?

(ii) What are the standards for creating and using agency declassification guides?

(iii) What is contained in the agency's automatic declassification plan?

(iv) What are the agency responsibilities for the maintenance of a declassification database?

(3) Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the creation or handling of classified information.

(i) What are the original and derivative classification processes and the standards applicable to each?

(ii) What are the proper and complete classification markings, as described in subpart B of this part?

(iii) What are the authorities, methods and processes for downgrading and declassifying information?

(iv) What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

(v) What are the requirements for creating and updating classification and declassification guides?

(vi) What are the requirements for controlling access to classified information?

(vii) What are the procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

(viii) What are the requirements for creating, maintaining, and terminating 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 G—Reporting and Definitions

§ 2001.80 Statistical reporting [5.2(b)(4)].

Each agency that creates or handles classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

§ 2001.81 Accounting for costs [5.4(d)(8)].

(a) Information on the costs associated with the implementation of the Order will be collected from the agencies. The agencies will provide data to ISOO on the cost estimates for classification-related activities. ISOO will report these cost estimates annually to the President. The agency senior official should work