

release the maximum information appropriate under the Freedom of Information Act (32 CFR part 285) and the interest of the Government in protecting the national security.

§ 159a.69 Scope and principles.

The security education program shall include all personnel authorized or expected to be authorized access to classified information. Each DoD Component shall design its program to fit the requirements of different groups of personnel. Care must be exercised to assure that the program does not evolve into a perfunctory compliance with formal requirements without achieving the real goals of the program. The program shall, as a minimum, be designed to:

(a) Advise personnel of the adverse effects to the national security that could result from unauthorized disclosure and of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control;

(b) Indoctrinate personnel in the principles, criteria, and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material, as prescribed in this Regulation, and alert them to the strict prohibitions against improper use and abuse of the classification system;

(c) Familiarize personnel with procedures for challenging classification decisions believed to be improper;

(d) Familiarize personnel with the security requirements of their particular assignment;

(e) Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information, and their responsibility to report such attempts;

(f) Advise personnel of the penalties for engaging in espionage activities;

(g) Advise personnel of the strict prohibition against discussing classified information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;

(h) Inform personnel of the penalties for violation or disregard of the provisions of this part (see § 159a.97(b));

(i) Instruct personnel that individuals having knowledge, possession, or control of classified information must determine, before disseminating such information, that the prospective recipient has been cleared for access by competent authority; needs the information in order to perform his or her official duties; and can properly protect (or store) the information.

§ 159a.70 Initial briefings.

DoD personnel granted a security clearance (see §159a.53) shall not be permitted to have access to classified information until they have received an initial security briefing and have signed Standard Form 189, "Classified Information Nondisclosure Agreement." DoD 5200.1-PH-1³⁵ provides a sample briefing and additional information regarding Standard Form 189. Cleared personnel employed prior to June 1, 1986 must sign Standard Form 189 as soon as practicable but not later than February 28, 1990.

§ 159a.71 Refresher briefings.

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in §159a.69 shall be tailored to fit the needs of experienced personnel.

§ 159a.72 Foreign travel briefings.

(a) Personnel who have had access to classified information shall be given a foreign travel briefing, before travel, to alert them to their possible exploitation under the following conditions:

(1) Travel to or through communist-controlled countries; and

(2) Attendance at international scientific, technical, engineering or other professional meetings in the United States or in any country outside the United States where it can be anticipated that representatives of Communist-controlled countries will participate or be in attendance. (See also DoD Directive 5240.6³⁶.)

(b) Individuals who travel frequently, or attend or host meetings of foreign visitors as described in paragraph (a)(2)

³⁵ See footnote 2 to § 159a.3

³⁶ See footnote 1 to § 159a.3.

§ 159a.73

of this section, need not be briefed for each occasion, but shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

§ 159a.73 Termination briefings.

(a) Upon termination of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

(1) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

(3) An acknowledgement that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

(4) An acknowledgement that the individual will report without delay to the FBI or the DoD Component concerned any attempt by any unauthorized person to solicit classified information.

(b) When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service who shall assure that it is recorded in the Defense Central Index of Investigations.

(c) The security termination statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's record retention schedules, but

32 CFR Ch. I (7-1-99 Edition)

for a minimum of 2 years after the individual is given a termination briefing.

Subpart L—Foreign Government Information

§ 159a.75 Classification.

(a) *Classification.* (1) Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a U.S. classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

(2) Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence must be classified by an original classification authority. The two-step procedure for classification prescribed in § 159a.15(c) does not apply to the classification of such foreign government information because E.O. 12356 states a presumption of damage to the national security in the event of unauthorized disclosure of such information. Therefore, foreign government information shall be classified at least Confidential, but higher whenever the damage criteria of § 159a.11 (b) or (c) are determined to be met.

(b) *Duration of Classification.* (1) Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

(2) Foreign government information classified by the Department of Defense under this or previous regulations shall be protected for an indefinite period (see § 159a.77(e)).

§ 159a.76 Declassification.

(a) *Policy.* In considering the possibility of declassification of foreign government information, officials shall respect the intent of this regulation to protect foreign government information and confidential foreign sources.