

§ 154.61

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

access to classified information is omitted.

(2) If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package.

I am aware of no information of the type contained at Appendix D, 32 CFR part 154, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information.

(3) If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

I am aware of information of the type contained in Appendix D, 32 CFR part 154, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s).

(4) In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs (c) (2) and (3) of this section as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

(d) *Individual responsibility.* (1) Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

(2) Moreover, individuals having access to classified information must report promptly to their security office:

(i) Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

(A) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(B) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

(ii) Any information of the type referred to in § 154.7 or appendix H to this part.

(e) *Co-worker responsibility.* Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61025, Nov. 19, 1993]

§ 154.61 Security education.

(a) *General.* The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, heads of DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

(b) *Initial briefing.* (1) All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this part shall be given an initial security briefing. The briefing shall be in accordance with the requirements of 32 CFR part 159 and consist of the following elements:

(i) The specific security requirements of their particular job.

(ii) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

(iii) The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

(iv) The penalties that may be imposed for security violations.

(2) If an individual declines to execute Standard Form 312, "Classified Information Nondisclosure Agreement" (replaced the Standard Form 189), the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with § 154.56(b).

(c) *Refresher briefing.* Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in 32 CFR part 159 shall be tailored to fit the needs of experienced personnel.

(d) *Foreign travel briefing.* While world events during the past several years have diminished the threat to our national security from traditional cold-war era foreign intelligence services, foreign intelligence service continue to pursue the unauthorized acquisition of classified or otherwise sensitive U.S. Government information, through the recruitment of U.S. Government employees with access to such information. Through security briefings and education, the Department of Defense continues to provide for the protection of information and technology considered vital to the national security interests from illegal or unauthorized acquisition by foreign intelligence services.

(1) DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office all contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

(i) Illegal or unauthorized access is sought to classified or otherwise sensitive information.

(ii) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

(2) The DoD security manager, security specialist or other qualified individual will review and evaluate the reported information. Any facts or circumstances of a reported contact with a foreign national that appear to:

(i) Indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified information or technology;

(ii) Offer a reasonable potential for such; or

(iii) Indicate the possibility of continued contact with the foreign national for such purposes, shall be promptly reported to the appropriate counterintelligence agency.

(e) *Termination briefing.* (1) 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:

(i) 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;

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

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

(iv) An acknowledgment 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.

(2) 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 ensure that it is recorded in the Defense Clearance and Investigations Index.

(3) 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 records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

(4) In addition to the provisions of paragraphs (e)(1), (e)(2), and (e)(3) of this section, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS-16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.

[52 FR 11219, Apr. 8, 1987, as amended at 58 FR 61026, Nov. 19, 1993]

Subpart J—Safeguarding Personnel Security Investigative Records

§ 154.65 General.

In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DoD military and civilian personnel, contractor employees, and other per-

sons affiliated with the Department of Defense, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counterintelligence investigations. Other uses are subject to the specific written authorization of the Deputy Under Secretary of Defense for Policy.

§ 154.66 Responsibilities.

DoD authorities responsible for administering the DoD personnel security program and all DoD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this part and that such reports and records are safeguarded as prescribed herein. The heads of DoD Components and the Deputy Under Secretary of Defense for Policy for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by §§ 154.67 and 154.68.

§ 154.67 Access restrictions.

Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with 32 CFR parts 286 and 286a and with the following:

(a) DoD personnel security investigative reports shall be released outside of the DoD only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

(b) Within DoD, access to personnel security investigative reports shall be limited to those designated DoD officials who require access in connection with specifically assigned personnel security duties, or other activities specifically identified under the provisions of § 154.65.

(c) Access by subjects of personnel security investigative reports shall be afforded in accordance with 32 CFR part 286a.

(d) Access to personnel security clearance determination information shall be made available, other than provided for in paragraph (c) of this