

on international treaty requirements (see DoD Directive 5100.55).

(b) The policies and procedures for access to and dissemination of Restricted Data and Critical Nuclear Weapon Design Information are contained in DoD Directive 5210.2.

(c) Special Access Programs for foreign intelligence information under the cognizance of the Director of Central Intelligence, or those of the National Telecommunications and Information Systems Security Committee originate outside the Department of Defense. However, coordination with the DUSD(P) and the Component's central point of contact is necessary before the establishment or implementation of any such Programs by any DoD Component. The information required by § 159a.80(f)(1) will be provided.

(d) Excluding those Programs and that information specified in paragraphs (a)(1), (2), and (3) of this section, Special Access Programs shall be established within the Military Departments by:

(1) Submitting to the Secretary of the Department the information required under § 159a.80(f)(1).

(2) Obtaining written approval from the Secretary of the Department;

(3) Providing to the DUSD(P) notice of the approval; and

(4) Maintaining the information and rationale upon which approval was granted within the Military Department's central office.

(e) Excluding those Programs and that information in paragraphs (d)(1), (2), and (3) of this section, Special Access Programs that are desired to be established in any DoD Component other than the Military Departments shall be submitted with the information referred to in § 159a.80(f)(1) to the DUSD(P) for approval.

(f) Upon specific written notice to one of the appropriate DoD Special Access Program approval officials, receipt of their written concurrence, protective Special Access Program controls may be applied to a prospective Special Access Program for up to a 6-month period from the date of such notice. However, in all instances, the Program must be terminated as a prospective Special Access Program or formally

approved as a Special Access Program by the end of the 6-month time period.

(g) Unless under DoD Directive S-5210.36³⁷, Special Access Programs which involve one or more DoD Components, or a DoD Component and a non-DoD activity, shall be covered by a written agreement which must document who has the principal security responsibility, who is the primary sponsor of the Program, and who is responsible for obtaining Special Access Program approval.

§ 159a.82 Review of special access programs.

(a) Excluding those Programs specified in § 159a.81 (a), (b), or (c), each Special Access Program shall be reviewed annually by the DoD Component responsible for establishment of the Program. To accommodate such reviews, DoD Components shall institute procedures to ensure the conduct of annual security inspections, with or without prior notice, and regularly scheduled audits by security, contract administration, and audit organizations. Also, Program managers shall ensure that Special Access Program activities have undergone a current review by legal counsel for compliance with law, executive order, regulation, and national policy. To accomplish such reviews, specially cleared pools of attorneys may be utilized, but in all cases legal counsel shall be provided with all information necessary to perform such reviews.

(b) Special Access Programs, excluding those specified in § 159a.81 (a), (b), or (c), or those required by treaty or international agreement, shall terminate automatically every 5 years unless reestablished in accordance with the procedures contained in § 159a.81.

§ 159a.83 Control and central office administration.

(a) Special Access Programs shall be controlled and managed in accordance with DoD Directive 5205.7³⁸. Each DoD Component shall appoint a Special Access Program coordinator to establish and maintain a central office and to serve as a single point of contact for

³⁷ See footnote 13 to § 159a.33(j).

³⁸ See footnote 1 to § 159a.3.

information concerning the establishment and security administration of all Special Access Programs established by or existing in the Component. These officials shall report to the DUSD(P) on the status of DoD Special Access Programs within the Component to include:

(1) The establishment of a Special Access Program as required by § 159a.81(d)(3); and

(2) Changes in Program status as required by § 159a.85 (b) or (c).

(b) Officials serving as single points of contact, as well as members of their respective staffs and other persons providing support to Special Access Programs who require access to multiple sets of particularly sensitive information, shall be subject to a counterintelligence-scope polygraph examination periodically but not less than once every 5 years. Additionally, such testing will be subject to the limitations imposed by Congress. The program for each DoD Component, as well as requests for waiver, shall be submitted for approval by the DUSD(P).

§ 159a.84 Codewords and nicknames.

Excluding those Programs specified in § 159a.81 (a), (b), and (c), each Special Access Program will be assigned a classified code word, or an unclassified nickname, or both. DoD Components other than Military Departments may request codewords and nicknames from the DUSD(P) individually or in block. If codewords or nicknames are obtained in block, however, the issuing Component shall promptly notify the DUSD(P) upon activation and assignment.

§ 159a.85 Reporting of special access programs.

(a) *Report of Establishment.* Reports to the Secretary of the Military Department or the DUSD(P) required under § 159a.81 for Special Access Programs shall include:

(1) The responsible department, agency, or DoD Component, including office identification;

(2) The codeword and/or nickname of the Program;

(3) The relationship, if any, to other Special Access Programs in the Depart-

ment of Defense or other government agencies;

(4) The rationale for establishing the Special Access Program including the reason why normal management and safeguarding procedures for classified information are inadequate;

(5) The estimated number of persons granted special access in the responsible DoD Component; other DoD Components; other government agencies; contractors; and the total of such personnel;

(6) A summary statement pertaining to the Program security requirements with particular emphasis upon those personnel security requirements governing access to Program information;

(7) The date of Program establishment;

(8) The estimated number and approximate dollar value, if known, of carve-out contracts that will be or are required to support the Program; and

(9) The DoD Component official who is the point of contact (last name, first name, middle initial; position or title; mailing address; and telephone number).

(10) A security plan and appropriate security classification guide and notification that a proper DD Form 254, "Contract Security Classification Specification," has been issued to contractors participating in the Program.

(b) *Annual Reports.* DoD Component annual reports from other than the Military Departments to the DUSD(P) shall be submitted not later than January 31 of each year, showing the changes in information provided under paragraph (a) of this section, as well as the date of last review. Annual reports shall reflect *actual* rather than *estimated* numbers of carve-out contracts and persons granted access and shall summarize the results of the inspections and audits required by § 159a.82(a). Reports from the Military Departments which have approval authority will summarize the required reviews which have been conducted during the year by the central offices, to include details and numbers of carve-out contracts associated with approved Special Access Programs and their overall security posture and numbers