

of approved Programs by type. Additionally, the Military Department Secretaries authorized to approve such Programs shall furnish a name listing, by unclassified nickname if practicable, or approved Special Access Programs under their cognizance, and they will report any changes to the listing as they occur pursuant to the notification requirements of § 159a.81(d)(3), that is, additions, deletions, and corrections to the DUSD(P). The effective date of information in the annual reports shall be December 31.

(c) *Termination Reports.* The DUSD(P) shall be notified upon termination of a Special Access Program.

§ 159a.86 Accounting for special access programs.

Each of the central offices which must be identified in accordance with § 159a.83(a) shall maintain a complete listing of currently approved DoD Special Access Programs which encompasses the information outlined in § 159a.85(a). These listings shall be readily available to the DUSD(P) or his designated representatives.

§ 159a.87 Limitations on access.

Access to data reported under this subpart shall be limited to the DUSD(P) and the minimum number of properly indoctrinated staff necessary to perform the functions assigned the DUSD(P) herein. Access may not be granted to any other person for any purpose without the approval of the DoD Components sponsoring the Special Access Programs concerned.

§ 159a.88 “Carve-Out” contracts.

(a) The Secretaries of the Military Departments and the DUSD(P), or their designees, shall ensure that, in those Special Access Programs involving contractors, special access controls are made applicable by legally binding instruments.

(b) To the extent necessary for DIS to execute its security responsibilities with respect to Special Access Programs under its security cognizance, DIS personnel shall have access to all information relating to the administration of these Programs.

(c) Excluding those Programs specified in § 159a.81(c), the use of “carve-out” contracts that relieve the DIS from inspection responsibility under the Defense Industrial Security Program is prohibited unless:

(1) Such contract supports a Special Access Program approved and administered under § 159a.81;

(2) Mere knowledge of the existence of a contract or of its affiliation with the Special Access Program is classified information; and

(3) Carve-out status is approved for each contract by the Secretary of a Military Department, the Director, NSA, the DUSD(P), or their designees.

(d) Approval to establish a “carve-out” contract must be requested from the Secretary of a Military Department, or designee(s), the Director, NSA, or designee(s), or in the case of other DoD Components, from the DUSD(P). Approved “carve-out” contracts shall be assured the support necessary for the requisite protection of the classified information involved. The support shall be specified through a system of controls that shall provide for:

(1) A written security plan, oral waivers of which are prohibited except in critical situations that must be documented as soon as possible after the fact.

NOTE: The plan must identify that DD Forms 254 have been distributed to the Defense Investigative Service as outlined in DoD Directive 5205.7.

(2) Professional security personnel at the sponsoring DoD Component performing security inspections at each contractor’s facility which shall be conducted, at a minimum, with the frequency prescribed by paragraph 4-103 of DoD 5220.22-R;

(3) “Carve-out” contracting procedures;

(4) A central office of record; and

(5) An official to be the single point of contact for security control and administration. DoD Components other than the Military Departments and NSA shall submit such appropriate rationale and security plan along with requests for approval to the DUSD(P).

(e) An annual inventory of carve-out contracts shall be conducted by each DoD Component which participates in Special Access Programs.

(f) This subsection relates back to the date of execution for each contract to which carve-out contracting techniques are applied. The carve-out status of any contract expires upon termination of the Special Access Program which it supports.

§ 159a.89 Oversight reviews.

(a) DUSD(P) shall conduct oversight reviews, as required, to determine compliance with this subpart.

(b) Pursuant to statutory authority, the Inspector General, Department of Defense, shall conduct oversight of Special Access Programs.

Subpart N—Program Management

§ 159a.91 Executive branch oversight and policy direction.

(a) *National Security Council.* Pursuant to the provisions of E.O. 12356, the NSC shall provide overall policy direction for the Information Security Program.

(b) *Administrator of General Services.* The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established under E.O. 12356. In accordance with E.O. 12356, the Administrator delegates the implementation and monitoring functions of the Program to the Director of the ISOO.

(c) *Information Security Oversight Office—(1) Composition.* The ISOO has a full-time director appointed by the Administrator of General Services with approval of the President. The Director has the authority to appoint a staff for the office.

(2) *Functions.* The Director of the ISOO is charged with the following principal functions that pertain to the Department of Defense:

(i) Oversee DoD actions to ensure compliance with E.O. 12356 implementing directives, for example, the ISOO Directive No. 1 and this part;

(ii) Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the Information Security Program;

(iii) Report annually to the President through the NSC on the implementation of E.O. 12356;

(iv) Review this Regulation and DoD guidelines for systematic declassification review; and

(v) Conduct on-site reviews of the Information Security Program of each DoD Component that generates or handles classified information.

(3) *Information Requests.* The Director of the ISOO is authorized to request information or material concerning the Department of Defense, as needed by the ISOO in carrying out its functions.

(4) *Coordination.* Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the ISOO are brought to the attention of the Director of Security Plans and Programs, ODUSD(P).

§ 159a.92 Department of Defense.

(a) *Management Responsibility.* (1) The DUSD(P) is the Senior DoD Information Security Authority having DoD-wide authority and responsibility to ensure effective and uniform compliance with and implementation of E.O. 12356 and its implementing ISOO Directive No. 1. As such, the DUSD(P) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The DUSD(P) or his designee may approve waivers or exceptions to the provisions of this part to the extent such action is consistent with E.O. 12356 and ISOO Directive No. 1.

(2) The heads of DoD Components may approve waivers to the provisions of this part only as specifically provided for herein.

(3) The Director, NSA/Chief, Central Security Service, under 32 CFR part 159, is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. In this regard, the Director, NSA, may approve waivers or exceptions to these special requirements. Except as provided in §159a.6 the authority to lower any COMSEC security standards rests with the Secretary of Defense. Requests for approval of such waivers or exceptions to established COMSEC security standards which, if adopted, will