

have the effect of lowering such standards, shall be submitted to the DUSD(P) for approval by the Secretary of Defense.

§ 159a.93 DoD components.

(a) *General.* The head of each DoD Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this part throughout the Component.

(b) *Military Departments.* In accordance with 32 CFR part 159 the Secretary of each Military Department shall designate a Senior Information Security Authority who shall be responsible for complying with and implementing this part within the Department.

(c) *Other Components.* In accordance with 32 CFR part 159, the head of each other DoD Component shall designate a Senior Information Security Authority who shall be responsible for complying with and implementing this Regulation within their respective Component.

(d) *Program Monitorship.* The Senior Information Security Authorities designated under paragraphs (b) and (c) of this section, are responsible within their respective jurisdictions for monitoring, inspecting with or without prior announcement, and reporting on the status of administration of the DoD Information Security Program at all levels of activity under their cognizance.

(e) *Field Program Management.* (1) Throughout the Department of Defense, the head of each activity shall appoint, in writing, an official to serve as security manager for the activity. This official shall be responsible for the administration of an effective Information Security Program in that activity with particular emphasis on security education and training, assignment of proper classifications, downgrading and declassification, safeguarding, and monitorship, to include sampling classified documents for the purpose of assuring compliance with this part.

(2) Activity heads shall ensure that officials appointed as security managers either possess, or obtain within a reasonable time after appointment, knowledge of and training in the Infor-

mation Security Program commensurate with the needs of their positions. The Director of Security Plans and Programs, ODUSD(P) shall, with the assistance of the Director, Defense Security Institute, develop minimum standards for training of activity security managers. Such training should result in appropriate certifications to be recorded in the personnel files of the individuals involved.

(3) Activity heads shall ensure that officials appointed as security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They also shall provide sufficient resources of time, staff, and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of the Information Security Program at all levels of the activity.

§ 159a.94 Information requirements.

(a) *Information Requirements.* DoD Components shall submit on a fiscal year basis a consolidated report concerning the Information Security Program of the Component on SF 311, "Agency Information Security Program Data," to reach the ODUSD(P) by October 20 of each year. SF 311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the ODUSD(P). The ODUSD(P) shall submit the DoD report (SF 311) to the ISOO by October 31 of each year. Interagency Report Control Number 0230-GSA-AN applies to this information collection system as well as to that contained in §159a.12.

§ 159a.95 Defense Information Security Committee.

(a) *Purpose.* The Defense Information Security Committee (DISC) is established to advise and assist the DUSD(P) and the Director, Security Plans and Programs (ODUSD(P) in the formulation of DoD Information Security Program policy and procedures.

(b) *Direction and Membership.* The DISC shall meet at the call of the DUSD(P) or the Director, Security Plans and Programs. It is comprised of the DUSD(P) as Chairman; the Director, Security Plans and Programs, as Vice Chairman; and the senior officials

(designated in accordance with section E.3.a., DoD Directive 5200.1,³⁹ or their representatives) responsible for directing and administering the Information Security Program of the OJCS, the Departments of the Army, Navy, and Air Force, the Defense Intelligence Agency, the Defense Nuclear Agency, the National Security Agency, and the Defense Investigative Service. Other DoD Components may be invited to attend meetings of particular interest to them.

Subpart O—Administrative Sanctions

§ 159a.97 Individual responsibility.

All personnel, civilian or military, of the Department of Defense are responsible individually for complying with the provisions of this part.

§ 159a.98 Violations subject to sanctions.

(a) DoD Military and civilian personnel are subject to administrative sanctions if they:

(1) Knowingly and willfully classify or continue the classification of information in violation of E.O. 12356, any implementing issuances, or this part.

(2) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12356 or prior orders; or

(3) Knowingly and willfully violate any other provision of E.O. 12356, any implementing issuances or this part.

(b) Sanctions include but are not limited to a warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge, and will be imposed upon any person, regardless of office or level of employment, who is responsible for a violation specified under this paragraph as determined appropriate under applicable law and DoD regulations. Nothing in this part prohibits or limits action under the Uniform Code of Military Justice based upon violations of that Code.

§ 159a.99 Corrective action.

The Secretary of Defense, the Secretaries of the Military Departments,

and the heads of other DoD Components shall ensure that appropriate and prompt corrective action is taken whenever a violation under § 159a.98(a) occurs or repeated administrative discrepancies or repeated disregard of requirements of this Regulation occur (see § 159a.100). Commanders and supervisors, in consultation with appropriate legal counsel, shall utilize all appropriate criminal, civil, and administrative enforcement remedies against employees who violate the law and security requirements as set forth in this part and other pertinent DoD issuances.

§ 159a.100 Administrative discrepancies.

Repeated administrative discrepancies in the marking and handling of classified information and material such as failure to show classification authority; failure to apply internal classification markings; failure to adhere to the requirements of this part that pertain to dissemination, storage, accountability, and destruction, and that are determined not to constitute a violation under § 159a.98(a) may be grounds for adverse administrative action including warning, admonition, reprimand or termination of classification authority as determined appropriate under applicable policies and procedures.

§ 159a.101 Reporting violations.

(a) Whenever a violation under § 159a.98(a)(2) occurs, the Director of Counterintelligence and Investigative Programs, ODUSD(P) shall be informed of the date and general nature of the occurrence including the relevant parts of this part, the sanctions imposed, and the corrective action taken. Whenever a violation under § 159a.98(a) (1) or (3) occurs, the Director of Security Plans and Programs, OSUSD(P) shall be provided the same information. Notification of such violations shall be furnished to the Director of the ISOO in accordance with § 5.4(d) of E.O. 12356 by the ODUSD(P).

(b) Any action resulting in unauthorized disclosure of properly classified information that constitutes a violation of the criminal statutes and evidence reflected in classified information of

³⁹See footnote 1 to § 159a.3