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 Information 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.

[39] See footnote 1 to § 159a.3