

that the regular incumbent is not serving in the position, a senior U.S. citizen official of the Commission listed in §60.4(a) will designate an eligible U.S. citizen to assume the duties and responsibilities of the position as set forth in this part.

(9) *Director, Office of Executive Administration*, “Deputy Director, Office of Executive Administration,” “Deputy Personnel Director,” and “Chief, Administrative Services,” are similarly defined to mean the U.S. citizen(s) temporarily designated to assume the responsibilities of the position as set forth in this part.

(10) *DUSD(P)* refers to the Deputy Under Secretary of Defense (Policy).

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§60.2 Compliance with Executive Order 12356 and implementing directives.

(a) The Director, Office of Executive Administration is designated the senior agency official to direct and administer the information security program for the Commission, including an active oversight and security education program to ensure effective implementation of Executive Order 12356 and any implementing directives published by the Information Security Oversight Office.

(b) The Director, Office of Executive Administration will establish procedures to prevent unnecessary access to classified information, including procedures that:

(1) Require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and

(2) Ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

(c) The Deputy Personnel Director will direct the conduct of investigations relative to the issuance of security clearances in accordance with the standards and criteria of Executive Order 10450.

[53 FR 7894, Mar. 11, 1988, as amended at 56 FR 59882, Nov. 26, 1991]

§60.3 Classification levels, categories, and limitations.

(a) Classification levels. Official information which requires protection against unauthorized disclosure in the interest of the national security shall be classified *Top Secret*, *Secret*, or *Confidential* depending upon the degree of its significance to national security. No other terms or phrases of classification shall be used to identify such information except as otherwise expressly provided by statute. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by one of the original classification authorities listed in §60.4(a), who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by one of the original classification authorities, who shall make this determination within thirty (30) days.

(1) *Top Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. The Commission does not have the authority to classify information originally as *Top Secret*.

(2) *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Classification categories. Information shall be considered for classification if it concerns:

(1) Military plans, weapons, or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities (including special activities), or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;