

## § 310.51

from certain designated provisions of the Act.

(2) Nothing in the Act permits exemption of any system of records from all provisions of the Act (see appendix D).

(b) *Establishing exemptions.* (1) Neither general nor specific exemptions are established automatically for any system of records. The head of the DoD Component maintaining the system of records must make a determination whether the system is one for which an exemption properly may be claimed and then propose and establish an exemption rule for the system. No system of records within the Department of Defense shall be considered exempted until the head of the Component has approved the exemption and an exemption rule has been published as a final rule in the FEDERAL REGISTER (see § 310.60(e), subpart G).

(2) Only the head of the DoD Component or an authorized designee may claim an exemption for a system of records.

(3) A system of records is considered exempt only from those provisions of the Privacy Act (5 U.S.C. 552a) which are identified specifically in the Component exemption rule for the system and which are authorized by the Privacy Act.

(4) To establish an exemption rule, see § 310.61 of subpart G.

(c) *Blanket exemption for classified material.* (1) Include in the Component rules a blanket exemption under 5 U.S.C. 552a(k)(1) of the Privacy Act from the access provisions (5 U.S.C. 552a(d)) and the notification of access procedures (5 U.S.C. 522a(e)(4)(H)) of the Act for all classified material in any system of records maintained.

(2) Do not claim specifically an exemption under section 552a(k)(1) of the Privacy Act for any system of records. The blanket exemption affords protection to all classified material in all systems of records maintained.

(d) *Provisions from which exemptions may be claimed.* (1) The head of a DoD Component may claim an exemption from any provision of the Act from which an exemption is allowed (see appendix D).

(2) Notify the Defense Privacy Office ODASD(A) before claiming an exemp-

## 32 CFR Ch. I (7-1-99 Edition)

tion for any system of records from the following:

(i) The exemption rule publication requirement (5 U.S.C. 552a(j)) of the Privacy Act.

(ii) The requirement to report new systems of records (5 U.S.C. 552a(o)); or

(iii) The annual report requirement (5 U.S.C. 552a(p)).

(e) *Use of exemptions.* (1) Use exemptions only for the specific purposes set forth in the exemption rules (see paragraph (b) of § 310.61, subpart G).

(2) Use exemptions only when they are in the best interest of the government and limit them to the specific portions of the records requiring protection.

(3) Do not use an exemption to deny an individual access to any record to which he or she would have access under the Freedom of Information Act (5 U.S.C. 552).

(f) *Exempt records in nonexempt systems.* (1) Exempt records temporarily in the hands of another Component are considered the property of the originating Component and access to these records is controlled by the system notices and rules of the originating Component.

(2) Records that are actually incorporated into a system of records may be exempted only to the extent the system of records into which they are incorporated has been granted an exemption, regardless of their original status or the system of records for which they were created.

(3) If a record is accidentally misfiled into a system of records, the system notice and rules for the system in which it should actually be filed will govern.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57800, Nov. 14, 1991]

### § 310.51 General exemptions.

(a) *Use of the general exemptions.* (1) No DoD Component is authorized to claim the exemption for records maintained by the Central Intelligence Agency established by 5 U.S.C. 552a(j)(1) of the Privacy Act.

(2) The general exemption established by 5 U.S.C. 552a(j)(2) of the Privacy Act may be claimed to protect investigative records created and maintained by law-enforcement activities of a DoD Component.

(3) To qualify for the (j)(2) exemption, the system of records must be maintained by an element that performs as its principal function enforcement of the criminal law, such as U.S. Army Criminal Investigation Command (CIDC), Naval Investigative Service (NIS), the Air Force Office of Special Investigations (AFOSI), and military police activities. Law enforcement includes police efforts to detect, prevent, control, or reduce crime, to apprehend or identify criminals; and the activities of correction, probation, pardon, or parole authorities.

(4) Information that may be protected under the (j)(2) exemption include:

(i) Records compiled for the purpose of identifying criminal offenders and alleged offenders consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, parole, and probation status (so-called criminal history records);

(ii) Reports and other records compiled during criminal investigations, to include supporting documentation.

(iii) Other records compiled at any stage of the criminal law enforcement process from arrest or indictment through the final release from parole supervision, such as presentence and parole reports.

(5) The (j)(2) exemption does not apply to:

(i) Investigative records prepared or maintained by activities without primary law-enforcement missions. It may not be claimed by any activity that does not have law enforcement as its principal function.

(ii) Investigative records compiled by any activity concerning employee suitability, eligibility, qualification, or for individual access to classified material regardless of the principal mission of the compiling DoD Component.

(6) The (j)(2) exemption claimed by the law-enforcement activity will not protect investigative records that are

incorporated into the record system of a nonlaw enforcement activity or into nonexempt systems of records (see paragraph (f)(2) of §310.50). Therefore, all system managers are cautioned to comply with the various regulations prohibiting or limiting the incorporation of investigatory records into system of records other than those maintained by law-enforcement activities.

(b) *Access to records for which a (j)(2) exemption is claimed.* Access to investigative records in the hands of a law-enforcement activity or temporarily in the hands of a military commander or other criminal adjudicative activity shall be processed under 32 CFR part 286, The DoD Freedom of Information Act Program, provided that the system of records from which the file originated is a law enforcement record system that has been exempted from the access provisions of this part (see paragraph (h) of §310.30, subpart D).

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57800, Nov. 14, 1991]

#### §310.52 Specific exemptions.

(a) *Use of the specific exemptions.* The specific exemptions permit certain categories of records to be exempted from certain specific provisions of the Privacy Act (see appendix D). To establish a specific exemption, the records must meet the following criteria (parenthetical references are to the appropriate subsection of the Privacy Act (5 U.S.C. 552a(k)):

(1) *The (k)(1).* Information specifically authorized to be classified under the DoD Information Security Program Regulation, 32 CFR part 159. (see also paragraph (c) of this section).

(2) *The (k)(2).* Investigatory information compiled for law-enforcement purposes by nonlaw enforcement activities and which is not within the scope of §310.51(a). If an individual is denied any right, privilege or benefit that he or she is otherwise entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This subsection when claimed allows limited protection