

§312.13

and possibly enable individuals to conceal their wrongdoing or mislead the course of the investigation by concealing, destroying or fabricating evidence or documents. Disclosures could also subject sources and witnesses to harassment or intimidation which jeopardize the safety and well-being of themselves and their families.

(6) From subsection (e)(1) because the nature of the investigation functions creates unique problems in prescribing specific parameters in a particular case as to what information is relevant or necessary. Due to close liaison and working relationships with other Federal, state, local, and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another government agency. It is necessary to maintain this information in order to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(7) From subsection (e)(4)(G) through (H) because this system of records is exempt from the access provisions of subsection (d).

(8) From subsection (f) because the agency's rules are inapplicable to those portions of the system that are exempt and would place the burden on the agency of either confirming or denying the existence of a record pertaining to a requesting individual might in itself provide an answer to that individual relating to an on-going investigation. The conduct of a successful investigation leading to the indictment of a criminal offender precludes the applicability of established agency rules relating to verification of record, disclosure of the record to that individual, and record amendment procedures for this record system.

[56 FR 51976, Oct. 17, 1991, as amended at 57 FR 24547, June 10, 1992; 61 FR 2916, Jan. 30, 1996]

§312.13 Ownership of OIG investigative records.

(a) Criminal and or civil investigative reports shall not be retained by DoD recipient organizations. Such reports are the property of OIG and are on loan to the recipient organization

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

for the purpose for which requested or provided. All copies of such reports shall be destroyed within 180 days after the completion of the final action by the requesting organization.

(b) Investigative reports which require longer periods of retention may be retained only with the specific written approval of OIG.

§312.14 Referral of records.

An OIG system of records may contain records other DoD Components or Federal agencies originated, and who may have claimed exemptions for them under the Privacy Act of 1974. When any action is initiated on a portion of any several records from another agency which may be exempt, consultation with the originating agency or component will be affected. Documents located within OIG system of records coming under the cognizance of another agency will be referred to that agency for review and direct response to the requester.

PART 313—THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF AND THE JOINT STAFF PRIVACY PROGRAM

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

§313.1 Source of regulations.

The Office of the Joint Chiefs of Staff is governed by the Privacy Act implementation regulations of the Office of the Secretary of Defense, 32 CFR part 311.

[40 FR 55535, Nov. 28, 1975. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57802, Nov. 14, 1991]

PART 314—DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, PRIVACY ACT OF 1974

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

§314.1 Source of regulations.

The Defense Advanced Research Projects Agency is governed by the

Office of the Secretary of Defense

§316.6

Privacy Act implementation regulations of the Office of the Secretary of Defense, 32 CFR part 311.

[40 FR 55535, Nov. 28, 1975. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57802, Nov. 14, 1991]

PART 315—UNIFORMED SERVICES UNIVERSITY OF HEALTH SCIENCES, PRIVACY ACT OF 1974

AUTHORITY: Pub. L. 93-579, 88 Stat. 1896 (5 U.S.C. 552a).

§315.1 Source of regulations.

The Uniformed Services University of the Health Sciences, is governed by the Privacy Act implementation regulations of the Office of the Secretary of Defense, 32 CFR part 311.

[40 FR 55535, Nov. 28, 1975. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57802, Nov. 14, 1991]

PART 316—DEFENSE INFORMATION SYSTEMS AGENCY PRIVACY PROGRAM

- Sec.
- 316.1 Purpose.
- 316.2 Applicability.
- 316.3 Authority.
- 316.4 Definitions.
- 316.5 Policy.
- 316.6 Procedures and responsibilities.
- 316.7 Questions.
- 316.8 Exemptions.

AUTHORITY: Pub. L. 93-579, 88 Stat. 1986 (5 U.S.C. 552a).

SOURCE: 40 FR 55535, Nov. 28, 1975, unless otherwise noted. Redesignated at 57 FR 6074, Feb. 20, 1992.

§316.1 Purpose.

This part delineates responsibility and provides guidance for the implementation of Pub. L. 93-579 (Privacy Act of 1974).

§316.2 Applicability.

This part applies to Headquarters, Defense Information Systems Agency (DISA) and DISA field activities.

[40 FR 55535, Nov. 28, 1975. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26389, May 14, 1997]

§316.3 Authority.

This part is published in accordance with the authority contained in 32 CFR part 310, August 1975.

[40 FR 55535, Nov. 28, 1975. Redesignated and amended at 57 FR 6074, Feb. 20, 1992]

§316.4 Definitions.

Add to the definitions contained in 32 CFR 310.6 the following:

System Manager: The DISA official who is responsible for policies and procedures governing a DISA System of Record. His title and duty address will be found in the paragraph entitled Sysmanager in DISA's Record System Notices which are published in the FEDERAL REGISTER in compliance with provisions of the Privacy Act of 1974.

[40 FR 55535, Nov. 28, 1975. Redesignated and amended at 57 FR 6074, Feb. 20, 1992; 62 FR 26389, May 14, 1997]

§316.5 Policy.

It is the policy of DISA:

(a) To preserve the personal privacy of individuals, to permit an individual to know what records exist pertaining to him in the DISA, and to have access to and have a copy made of all or any portion of such records and to correct or amend such records.

(b) To collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

[40 FR 55535, Nov. 28, 1975. Redesignated at 57 FR 6074, Feb. 20, 1992, as amended at 62 FR 26389, May 14, 1997]

§316.6 Procedures and responsibilities.

(a) The Counsel, DISA, is hereby designated the Privacy Act Officer for DISA and is responsible for insuring that an internal DISA Privacy Program is established and maintained. He will also insure that all echelons of DISA effectively comply with and implement 32 CFR part 310.

(b) The Civilian Assistant to the Chief of Staff will be responsible for